CHFI v9 - CEH VIETNAM

Hiểu về nghiệp vụ điều tra pháp y số kỹ thuật số

Khóa học : https://akademy.edu.vn/course/chuong-trinh-dao-tao-chfi-v9/

Giới thiệu

Các **bài học tìm** Hiểu về nghiệp vụ điều tra pháp y số kỹ thuật số

Lưu ý : Trong bài hướng dẫn thực hành chúng tôi soạn và dịch cả những menu hay button hoặc tên hộp thoại sang tiếng Việt, vì vậy các bạn cần có kiến thức tiếng Anh ở mức cơ bản để có thể hiểu Tệp là File, Save là lưu hay Mở là Open ... Nếu gặp khó khăn hãy xem hình minh họa kèm theo để thấy tên gốc bằng tiếng Anh.

Phòng thí nghiệm trực tuyến Secuirty365 – Practice Labs sẽ cung cấp cho bạn với các hướng dẫn và các thiết bị thật để phát triển kỹ năng nghề nghiệp như một điều tra viên trong lĩnh vực máy tính và dữ liệu số trong các chủ đề sau.

- Có được hình ảnh của bằng chứng qua các biện pháp thu thập chứng cứ số
- Phân tích bằng chứng kỹ thuật số của bạn
- Dự án thực hành 1-1
- Dự án thực hành 1-2
- Dự án thực hành 1-3
- Dự án thực hành 1-4
- Dự án thực hành 1-5
- Dự án thực hành 1-6

Sơ đồ phòng thí nghiệm online

Trong phiên học tập của bạn, bạn sẽ có quyền truy cập vào cấu hình lab sau. Tùy thuộc vào các bài tập, bạn có thể sử dụng hoặc không sử dụng tất cả các thiết bị, nhưng chúng được hiển thị trong bố cục để hiểu tổng thể về cấu trúc liên kết của phòng thí nghiệm online.



Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo

Kết nối với Phòng thí nghiệm của bạn

Trong mô-đun này, bạn sẽ làm việc trên các thiết bị sau đây để thực hiện các bước được xác định trong mỗi bài tập.

- **PLABWIN810** (Máy trạm Windows 8.1)

Mỗi bài tập sẽ trình bày các chi tiết bạn cần sử dụng thiết bị nào để thực hiện các bước thực tập.

Để bắt đầu, chỉ cần nhấp vào Máy chủ hoặc Máy trạm đã đặt tên từ danh sách thiết bị (nằm ở bên trái màn hình) và nhấp **vào** biểu tượng Bật nguồn từ thanh công cụ. Trong một số trường hợp, thiết bị có thể tự động bật nguồn. Nếu bạn sử dụng mô hình lab ofline (chạy trên máy tính thì phải cài đặt các thiết bị trên với khá nhiêu công đoạn)

Trong quá trình khởi động, một chỉ báo hoạt động sẽ được hiển thị trong tab tên thiết bị:

- Đen (Black) - Đã tắt nguồn
- Màu xah da trời (Blue) - Làm việc theo yêu cầu của bạn
- Màu xanh lá cây (Green) - Sẵn sàng truy cập

Nếu thiết bị đầu cuối từ xa không được hiển thị tự động trong cửa sổ chính (hoặc cửa sổ bật lên), hãy nhấp vào biểu tượng Kết nối nằm trong thanh công cụ để bắt đầu phiên của bạn.

Nếu bảng điều khiển từ xa không xuất hiện, vui lòng thử tùy chọn sau:

- Chuyển đổi giữa các phiên bản máy khách HTML 5 và Java trong thanh công cụ. Nên sử dụng trình duyệt Chrome để có trãi nghiệm tốt nhất

Trong trường hợp điều này không giải quyết được sự cố kết nối của bạn, vui lòng truy cập trang Trợ giúp / Hỗ trợ của chúng tôi qđể biết thêm các tùy chọn giải quyết. Hoặc liên hệ với các Admin

Bài tập 1 – Thu thập Bằng chứng số

Sau khi bạn truy xuất và bảo đảm an toàn bằng chứng số theo quy trình của điều tra sốo, bạn đã sẵn sàng sao chép phương tiện bằng chứng và phân tích dữ liệu. Quy tắc đầu tiên của pháp y số là bảo tồn bằng chứng ban đầu. Sau đó, chỉ tiến hành phân tích trên bản sao dữ liệu — hình ảnh của phương tiện gốc. Một số nhà cung cấp   các công cụ trên MS-DOS, Linux và Windows. Tuy nhiên, các công cụ Windows yêu cầu thiết bị chặn ghi (được thảo luận trong Chương 3) khi lấy dữ liệu từ hệ thống tệp FAT hoặc NTFS.

Nhiệm vụ 1 - Sử dụng ProDiscover Basic để lấy ảnh ổ đĩa

ProDiscover Basic from Technology Pathways là một công cụ phân tích pháp y số. Bạn có thể sử dụng nó để thu thập và phân tích dữ liệu từ một số hệ thống tệp khác nhau, chẳng hạn như Microsoft FAT và NTFS; Linux Ext2, Ext3 và Ext4; và các hệ thống tệp UNIX khác, từ Windows XP hoặc HĐH cũ hơn.

Quan trọng : ProDiscover Basic 64 đã được cài đặt sẵn trên thiết bị **PLABWIN810** trong phòng thí nghiệm này. DVD kèm theo cuốn sách này bao gồm ProDiscover Basic. Chương trình cài đặt bao gồm sách hướng dẫn sử dụng, ProDiscoverManual.pdf, trong thư mục **C: \ Program Files \ (x86) \ Technology Pathways \ ProDiscover** (nếu sử dụng mặc định cài đặt; đối với HĐH Windows cũ hơn, hãy tìm trong C: \ Program Files \ Thư mục \ TechnologyPathways \ ProDiscover). Đọc hướng dẫn sử dụng để biết hướng dẫn và cài đặt ProDiscover Basic trên máy tính của bạn trước khi bạn thực hiện hoạt động sau. Trong Windows Vista trở lên, bạn phải ở chế độ Quản trị viên.

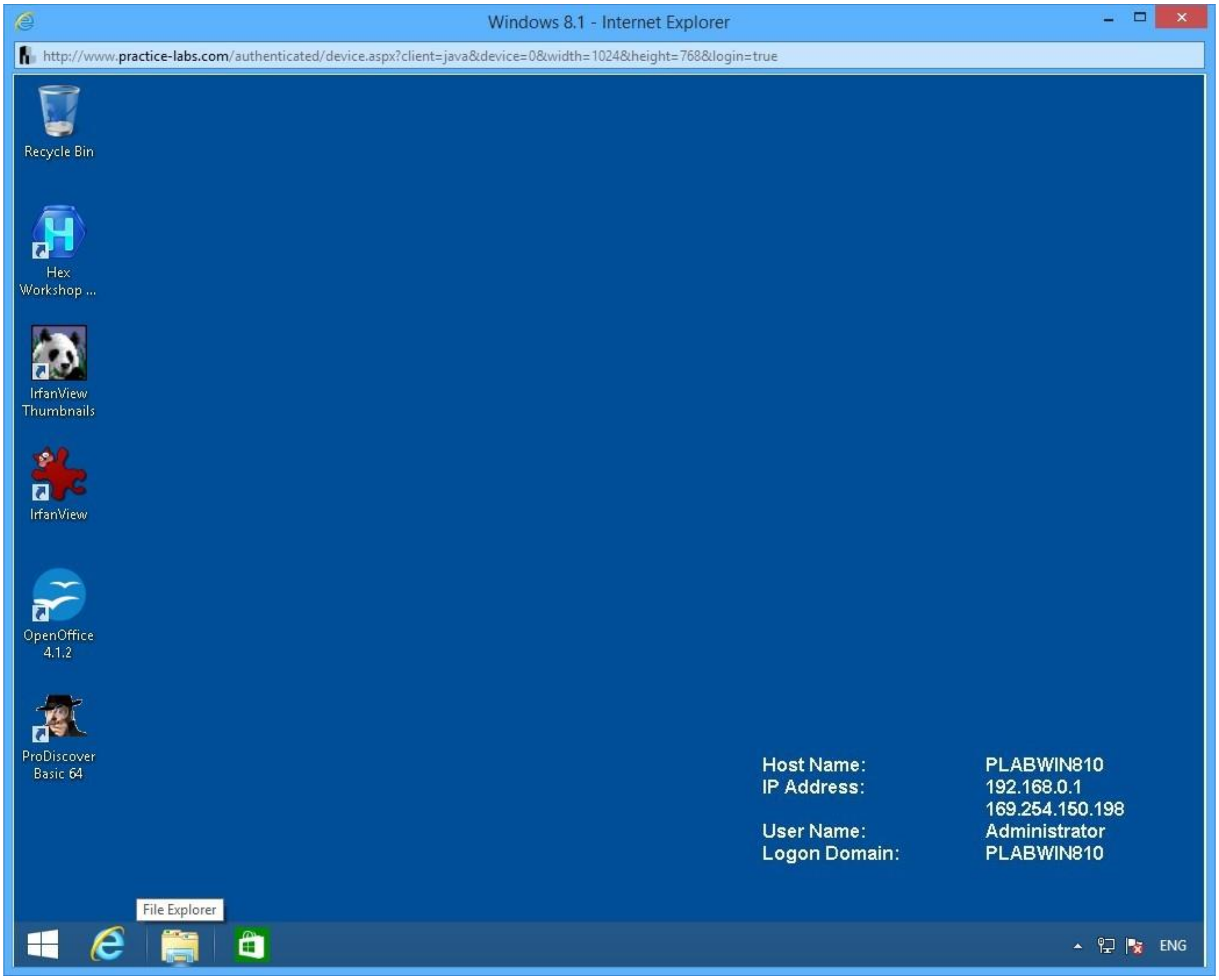
Để bắt đầu sử dụng ProDiscover lấy hình ảnh đĩa, hãy làm theo các bước sau:

Bước 1

Đảm bảo rằng bạn đã cấp nguồn cho thiết bị cần thiết được chỉ ra trong phần Giới thiệu của phòng thí nghiệm này (nhấn nút Power On)

Kết nối với thiết bị **PLABWIN810** .

Khi đã đăng nhập, hãy nhấp vào biểu tượng **File Explorer** trên thanh tác vụ.



Bước 2

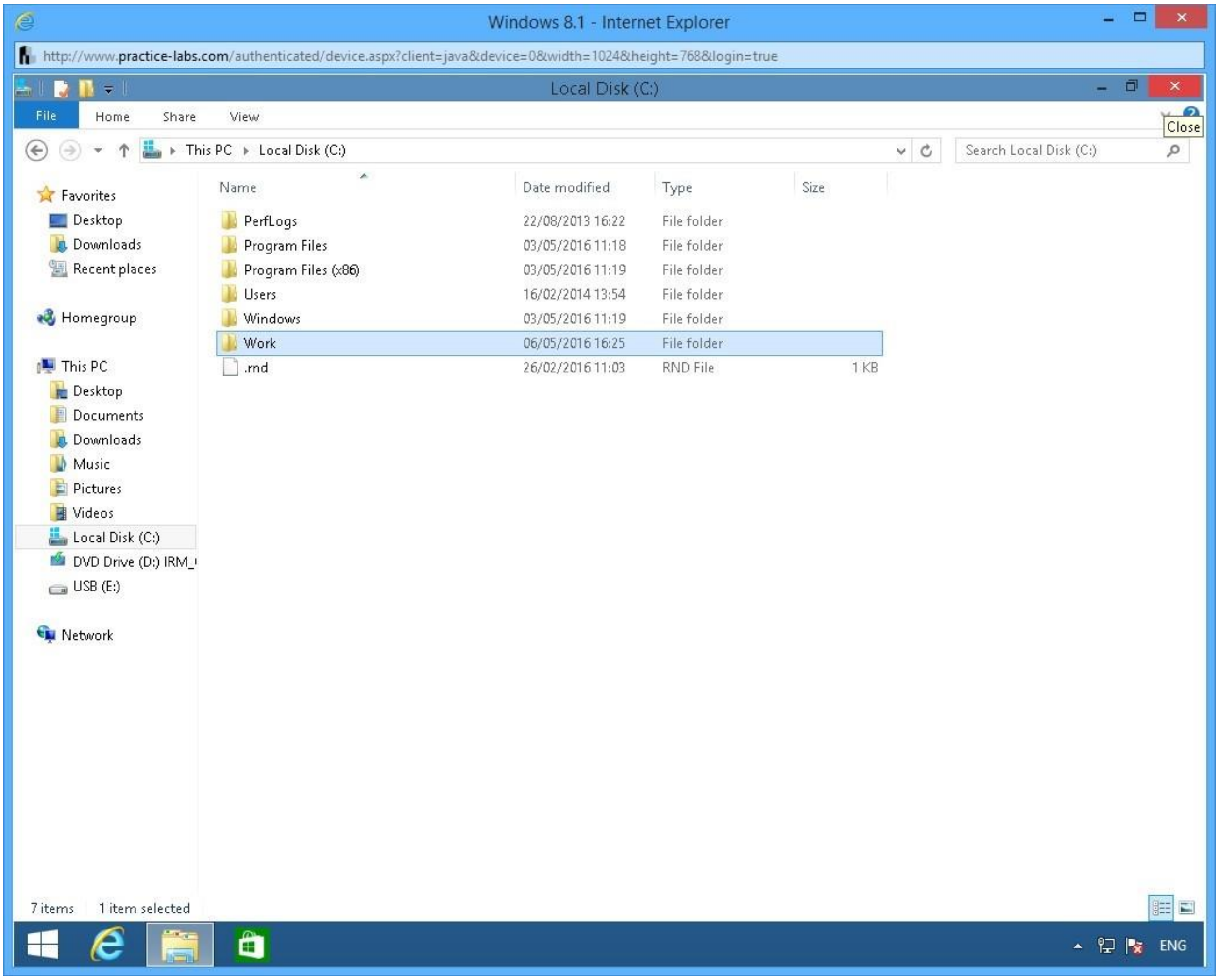
Điều hướng đến vị trí sau:

```
C:\Work
```

Thư mục này sẽ được sử dụng để lưu trữ dữ liệu và các tệp liên quan khác mà ProDiscover tạo ra khi thu thập và phân tích bằng chứng.

Lưu ý: *Bạn có thể sử dụng bất kỳ vị trí và tên nào cho thư mục công việc của mình, nhưng bạn sẽ thấy nó được gọi trong các hoạt động là "C: \ Work" hoặc đơn giản là thư mục công việc của bạn*

Đóng cửa sổ **File Explorer** .



Bước 3

Các bước sau đây sẽ chỉ ra cách lấy ảnh của ổ đĩa E được gọi là USB. Xin lưu ý rằng ổ này không phải là ổ USB thực tế mà là ổ cố định trên máy tính.

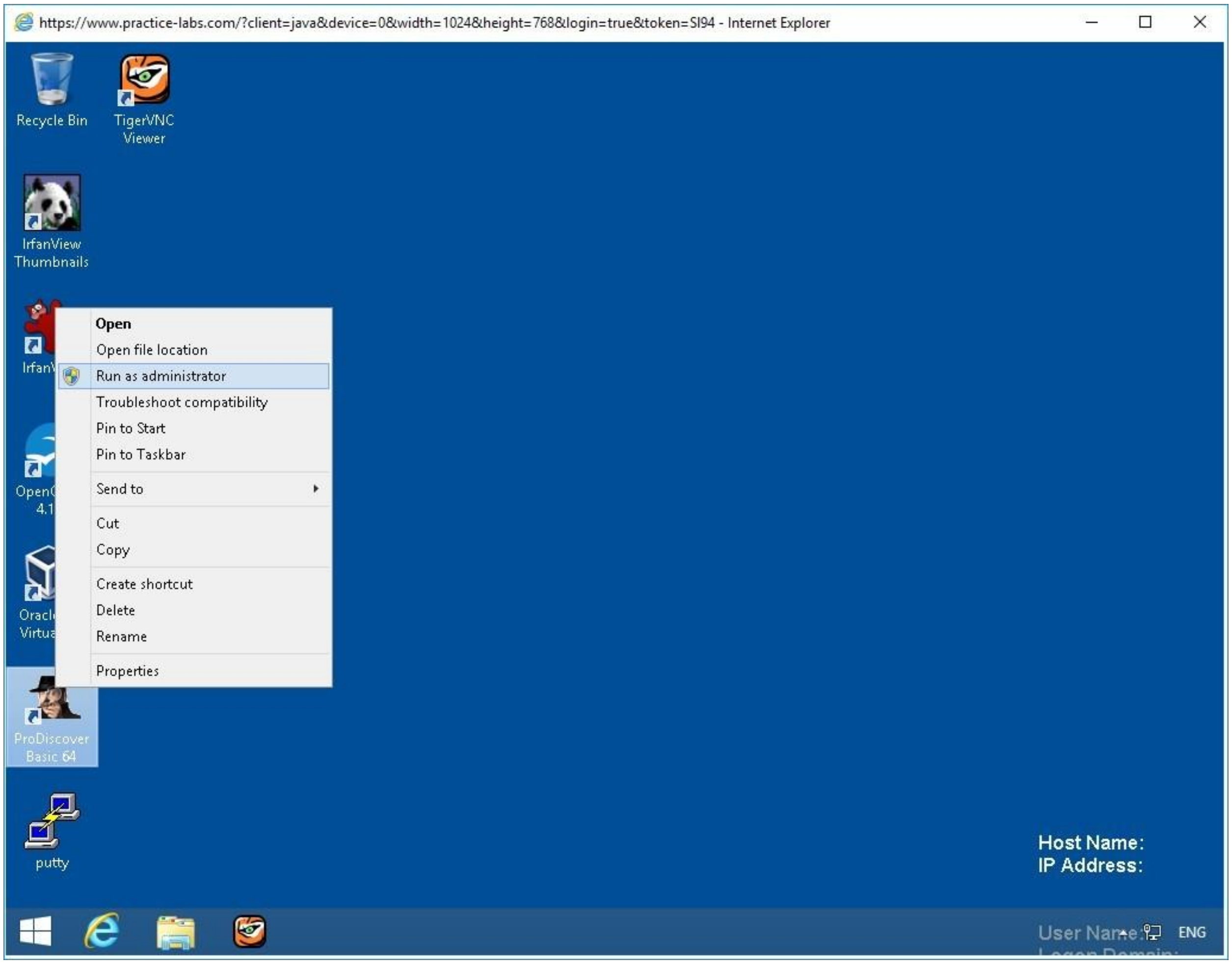
Việc thu thập hình ảnh có thể được áp dụng các phương tiện khác, chẳng hạn như ổ đĩa cố định và lưu trữ cổng thông tin như ổ đĩa flash USB.

***Lưu ý** : Trên ổ USB, tìm công tắc chống ghi (nếu có) và đặt ổ ở chế độ chống ghi. Sau đó, kết nối ổ USB với máy tính của bạn. (Hầu hết các ổ flash USB hiện tại không có công tắc chặn ghi; đối với hoạt động này, người ta cho rằng ổ flash USB đã được bảo vệ chống ghi.) Hoạt động này nhằm giới thiệu cho bạn công cụ ProDiscover Basic. Các thủ tục pháp y số thích hợp yêu cầu bảo vệ bằng văn bản bất kỳ phương tiện bằng chứng nào để đảm bảo rằng nó không bị thay đổi.*

Bước 4

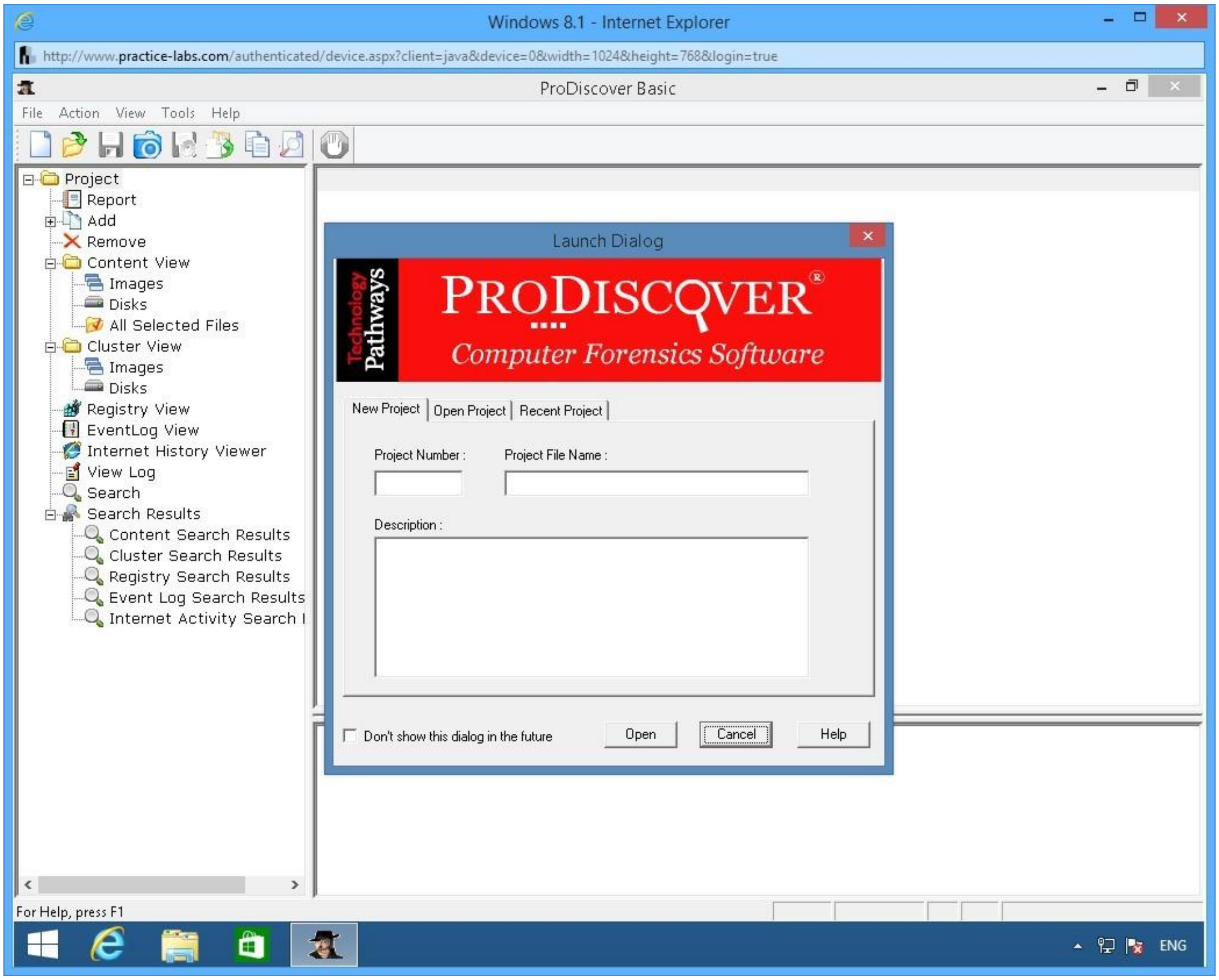
Khởi động **ProDiscover Basic** với **quyền Quản trị** .

*Để Open **ProDiscover Basic** với quyền Quản trị, nhấp chuột phải vào lối tắt trên màn hình và chọn **Chạy với tư cách Quản trị viên** . Bạn sẽ cần nhấn Có trên hộp Kiểm soát Tài khoản Người dùng.*



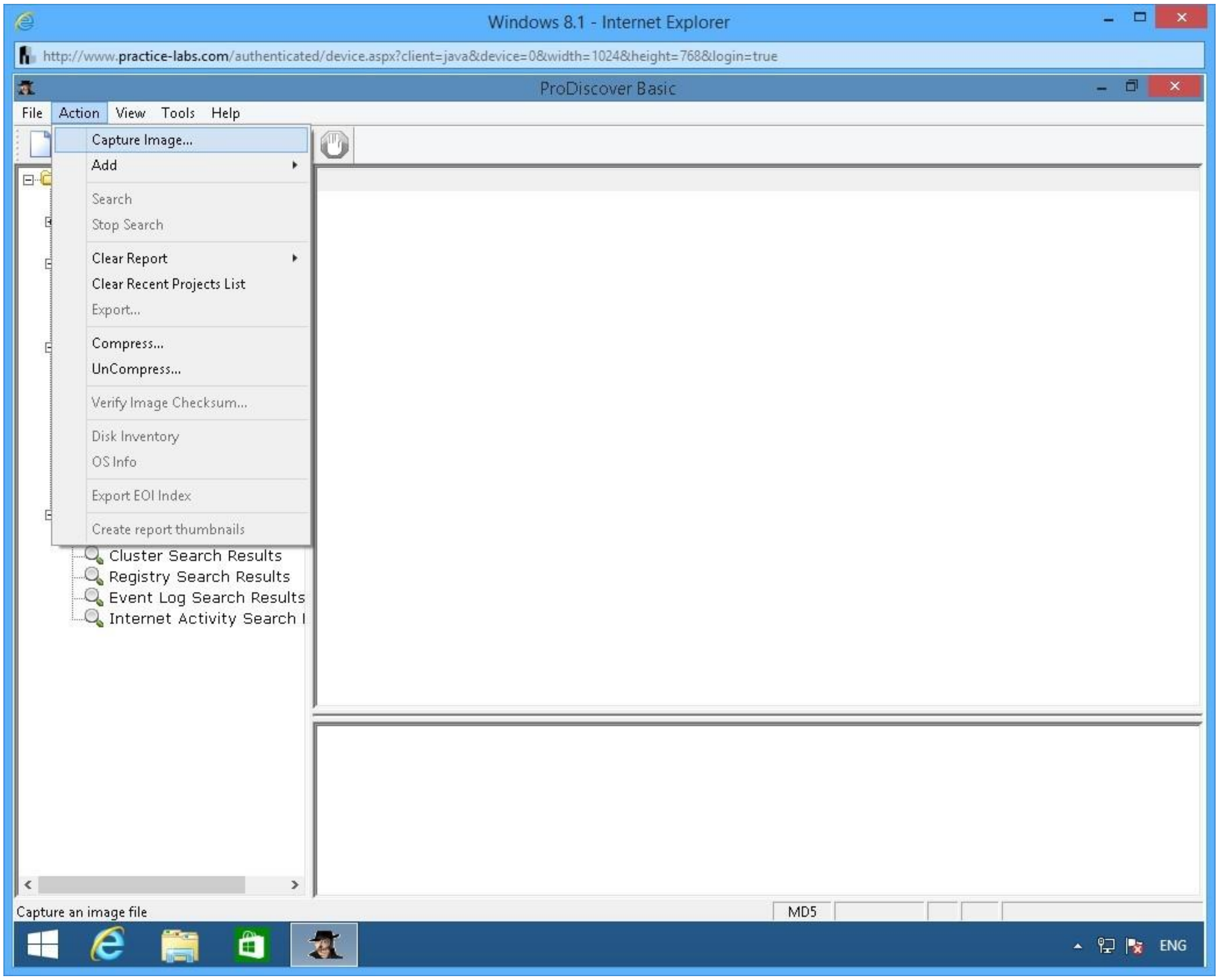
Bước 5

Nếu hộp thoại khởi chạy **ProDiscover** Open ra, hãy nhấp vào **Hủy** .



Bước 6

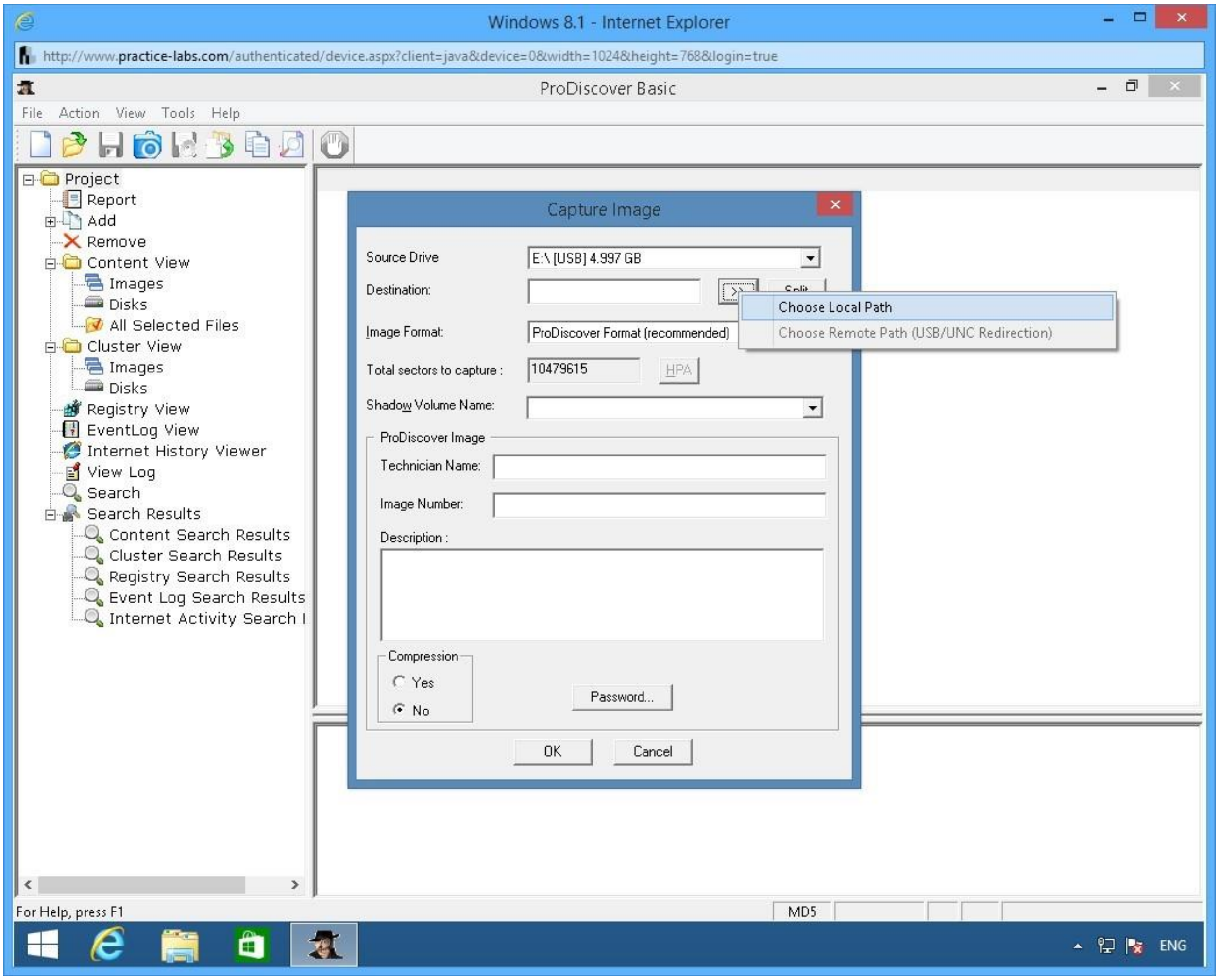
Trong cửa sổ chính, nhấp vào menu **Hành động** (Action) , nhấp vào **Chụp ảnh (Capture Image)** .



Bước 7

Trong hộp thoại Capture Image, nhấp vào mũi tên danh sách **Ổ nguồn** (source Drive) và chọn ổ **E: \ [USB] 4.997 GB** .

Nhấp vào nút **>>** bên cạnh hộp văn bản **Đích** và nhấp vào **Chọn Đường dẫn Địa phương** (Choose Local Path).



Bước 8

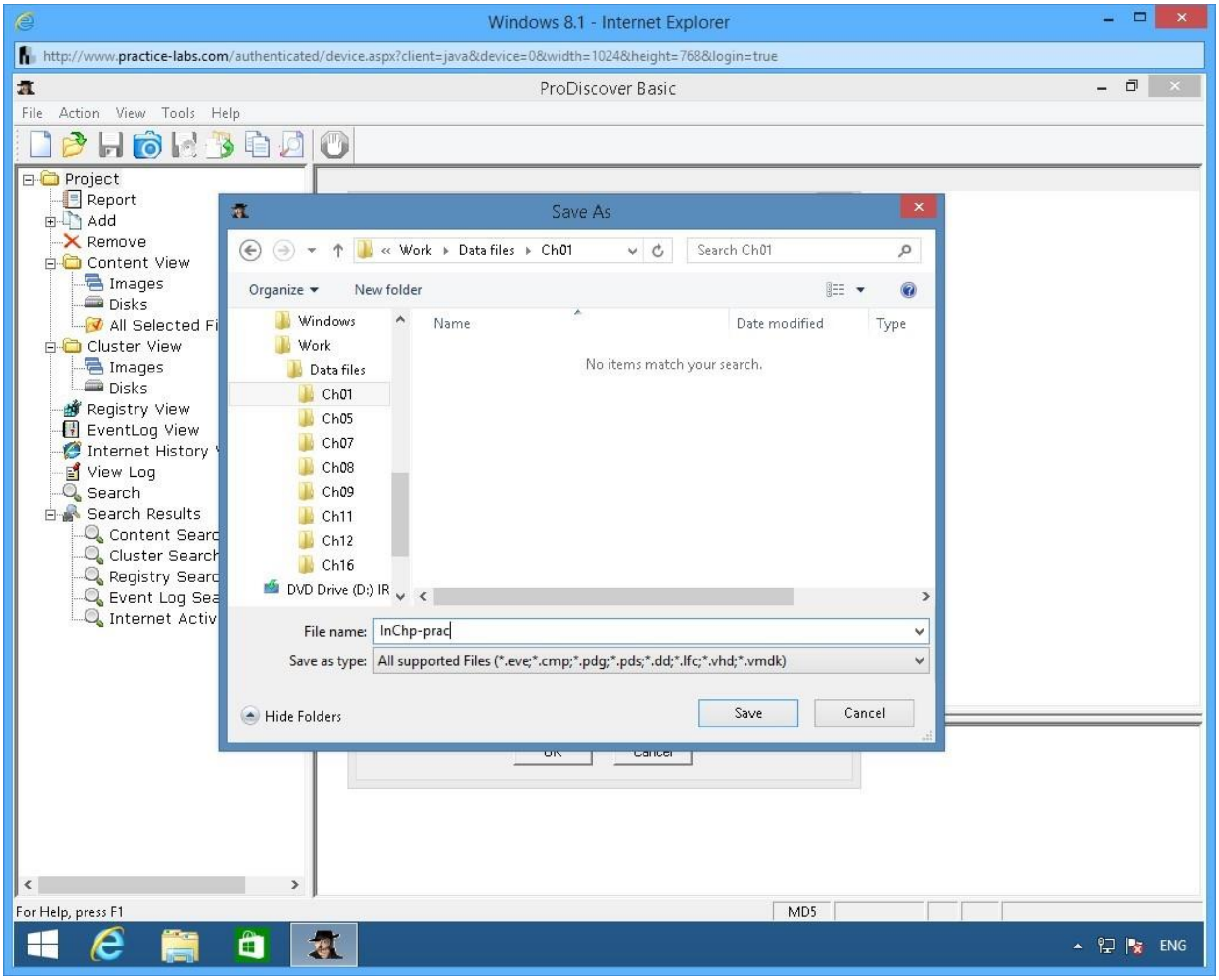
Khi hộp thoại **Save As** Open ra, hãy Mở rộng **Local Disk (C :)> Work> Data files,** sau đó nhấp vào thư mục **Ch01** .

Nhập tên cho hình ảnh bạn đang tạo, chẳng hạn như:

```
InChp-prac
```

Nhấp vào **Lưu** (Save) để lưu tệp.

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



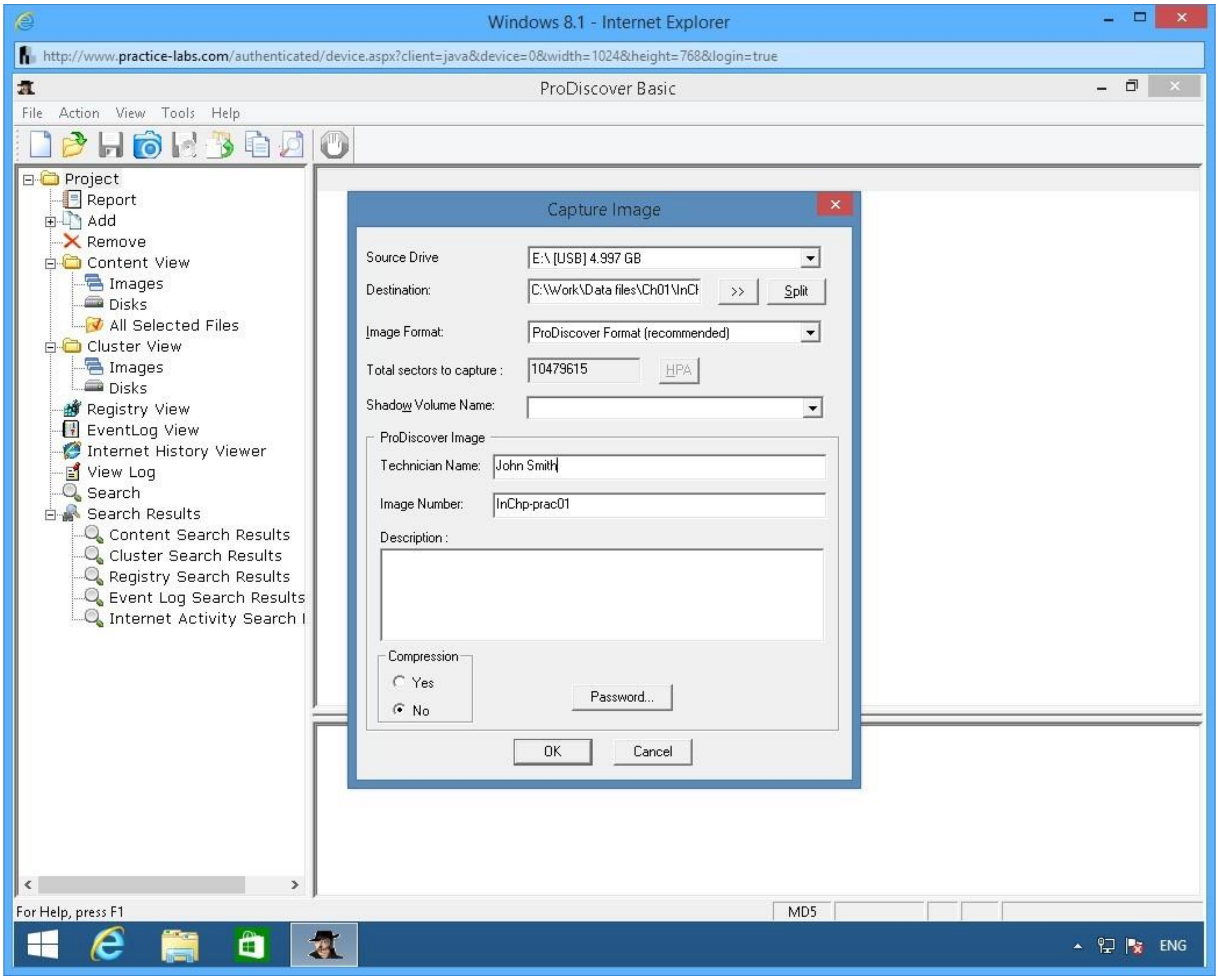
Bước 9

Quay lại hộp thoại Capture Image, nhập tên của bạn vào hộp văn bản **Tên kỹ thuật viên** (Technician Name, ví dụ John Smith hay tên của bạn).

Trong hộp văn bản **Số Hình ảnh** (Image Number), hãy nhập:

```
InChp-prac01
```

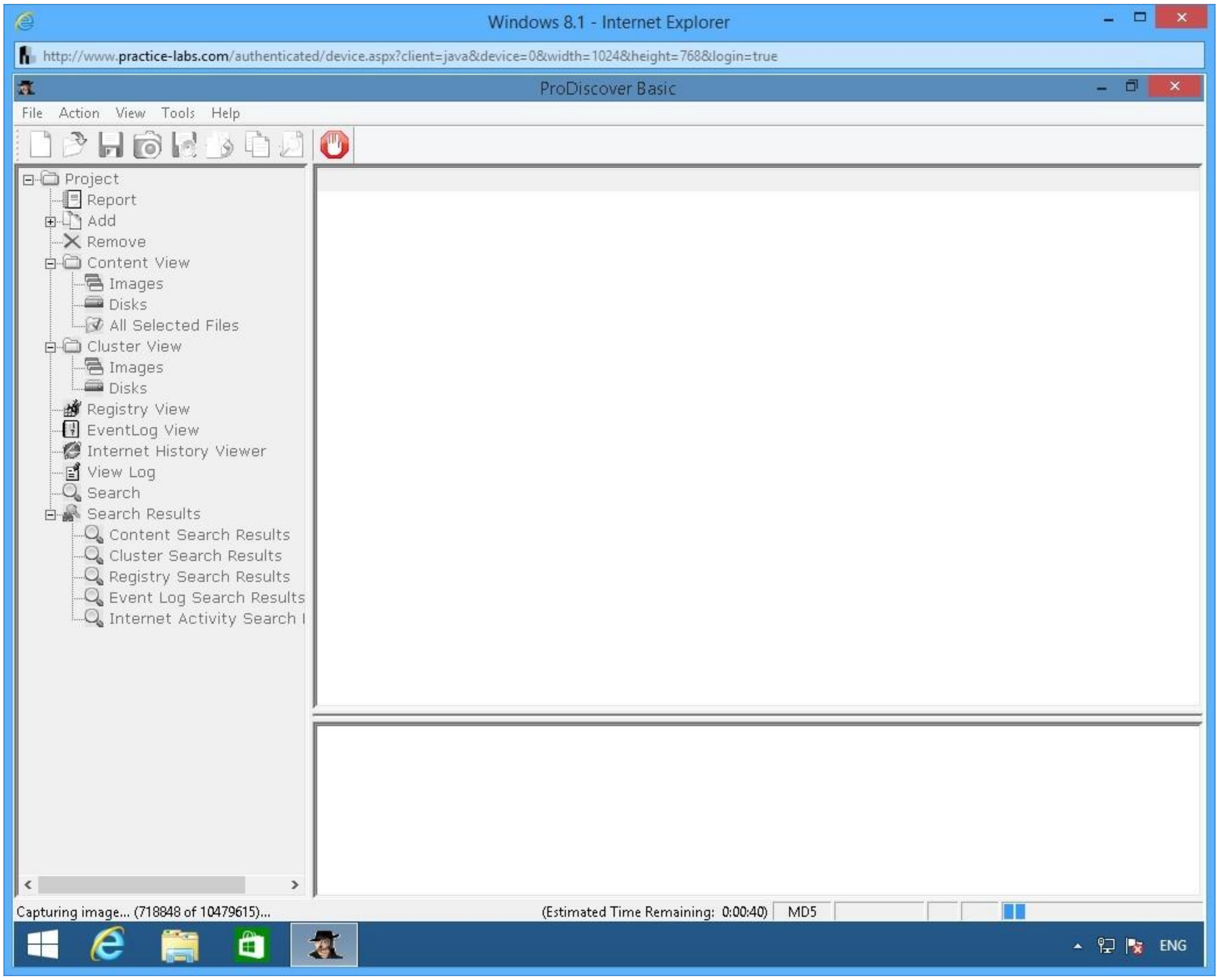
Bấm **OK** .



Bước 10

Sau đó, ProDiscover Basic sẽ thu hình ảnh của ổ đĩa đích như bạn có thể thấy từ trạng thái của ổ đĩa đang chụp ở cuối cửa sổ.

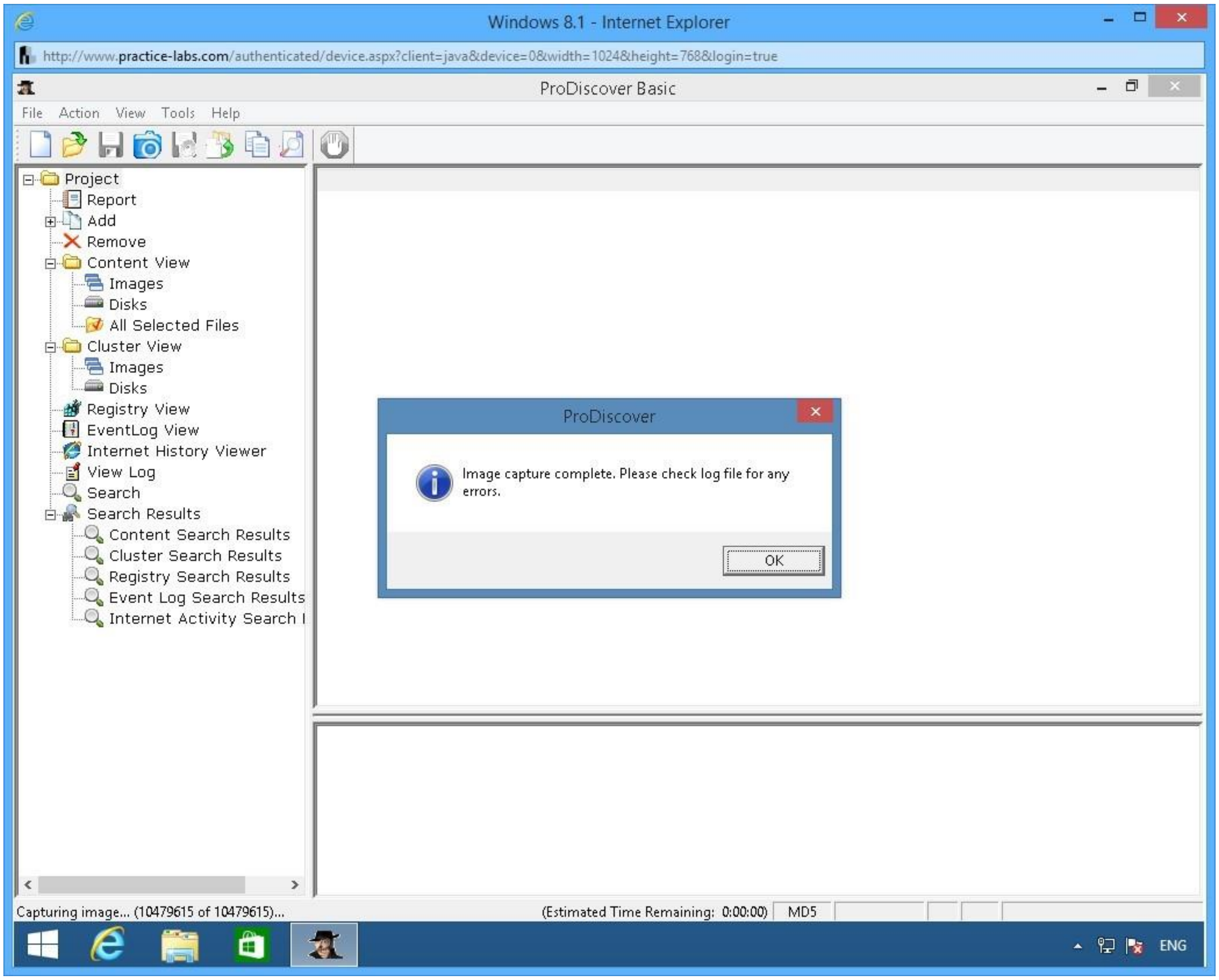
Vui lòng đợi vì quá trình này sẽ mất vài giây.



Bước 11

Khi hoàn tất, nó sẽ hiển thị thông báo để kiểm tra tệp nhật ký được tạo trong quá trình chuyển đổi. Tệp nhật ký này chứa thông tin bổ sung nếu gặp lỗi trong quá trình thu thập dữ liệu. ProDiscover cũng tạo tệp đầu ra băm MD5. Trong Chương 3 và 4, bạn học cách sử dụng MD5 để phân tích pháp y số và xác thực bằng chứng.

Khi ProDiscover kết thúc, bấm **OK** trong hộp thông báo hoàn thành.

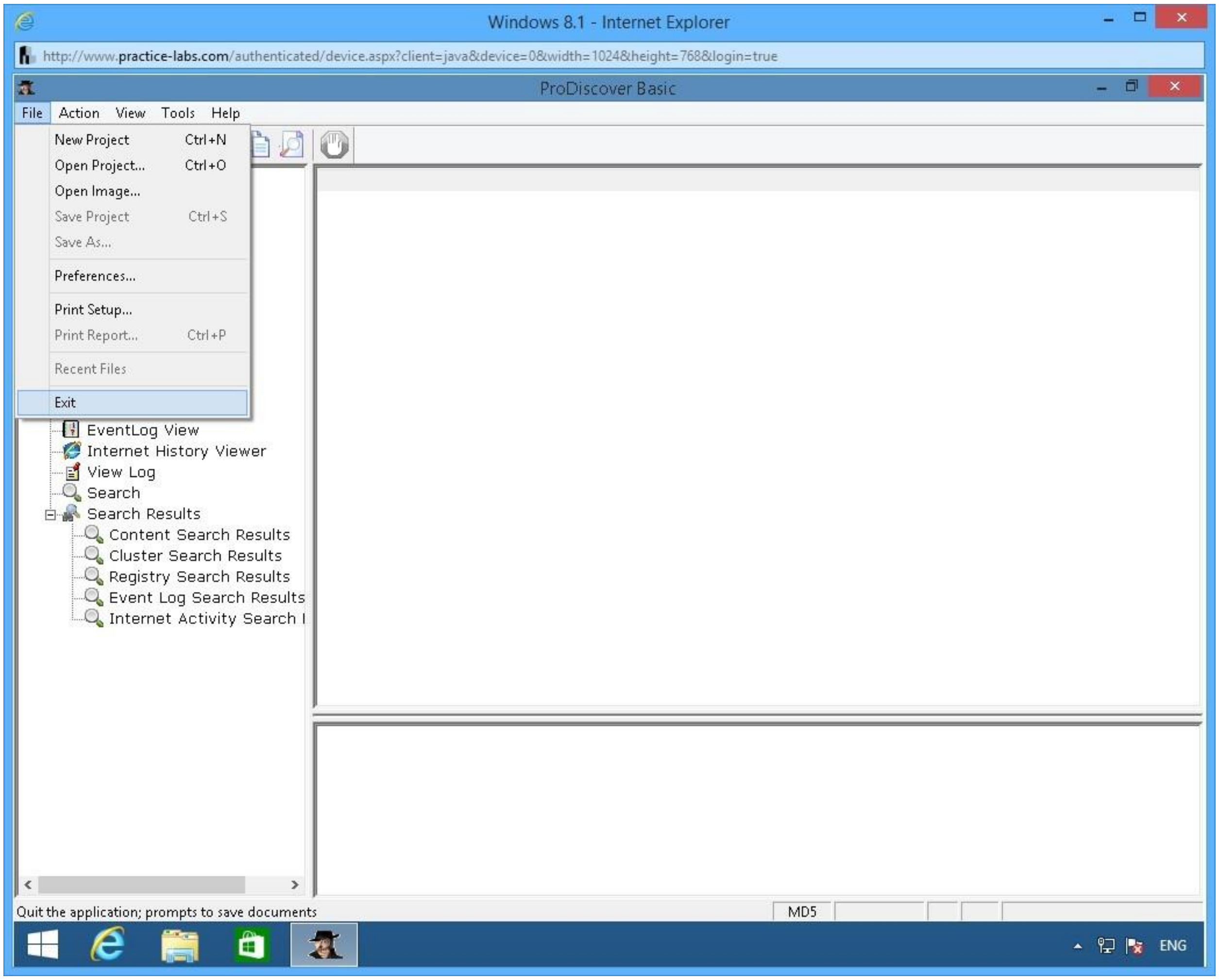


Bước 12

Nhấp vào **Tệp** (File) , chọn **Thoát** (Exit) từ menu để thoát khỏi ProDiscover.

Hoạt động này hoàn thành việc thu thập dữ liệu pháp y số đầu tiên của bạn. Tiếp theo, bạn học cách xác định vị trí dữ liệu trong chuyển đổi.

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Giữ cho thiết bị được bật nguồn ở trạng thái hiện tại và tiến hành bài tập tiếp theo.

Lưu ý : Trong Bài tập 1 BQT có ghi kèm một số thuật ngữ hay nghĩa tiếng Anh gốc của menu hay giao diện hiển thị của ứng dụng, còn về sau thì các bạn hãy tự hiểu ví dụ Tệp sẽ tương ứng với File, Exit là Thoát ... Hãy ghi nhớ tất cả những thuật ngữ cơ bản trong môi trường IT này.

Bài tập 2 - Phân tích bằng chứng kỹ thuật số của bạn

Khi bạn phân tích bằng chứng kỹ thuật số, công việc trước tiên của bạn là khôi phục dữ liệu. Nếu người dùng đã xóa hoặc ghi đè các tệp trên đĩa, đĩa sẽ chứa các tệp đã xóa và các đoạn tệp ngoài các tệp hiện có. Hãy nhớ rằng khi các tệp bị xóa, không gian chúng chiếm sẽ trở thành không gian trống — nghĩa là nó có thể được sử dụng cho các tệp mới được lưu hoặc các tệp Mở rộng khi dữ liệu được thêm vào chúng.

Các tệp đã bị xóa vẫn còn trên đĩa cho đến khi một tệp mới được lưu vào cùng một vị trí thực, ghi đè lên tệp gốc. Trong thời gian chờ đợi, những tệp đó vẫn có thể được truy xuất. Các công cụ pháp y số như ProDiscover Basic có thể truy xuất các tệp đã xóa để sử dụng làm bằng chứng.

Tuy nhiên, theo kinh nghiệm của tôi thì ta nên mount ảnh đĩa hay phươn tiện bằng chứng được thu thập vào hệ thống Forensic Lab rồi dùng các tool chuyên dụng như Easy US Data Recovery để tiến trình khôi mục diễn ar mạnh mẽ nhất. Đó cũng là bài thực hành trong chương dầu tiên của giáo trình CHFI.

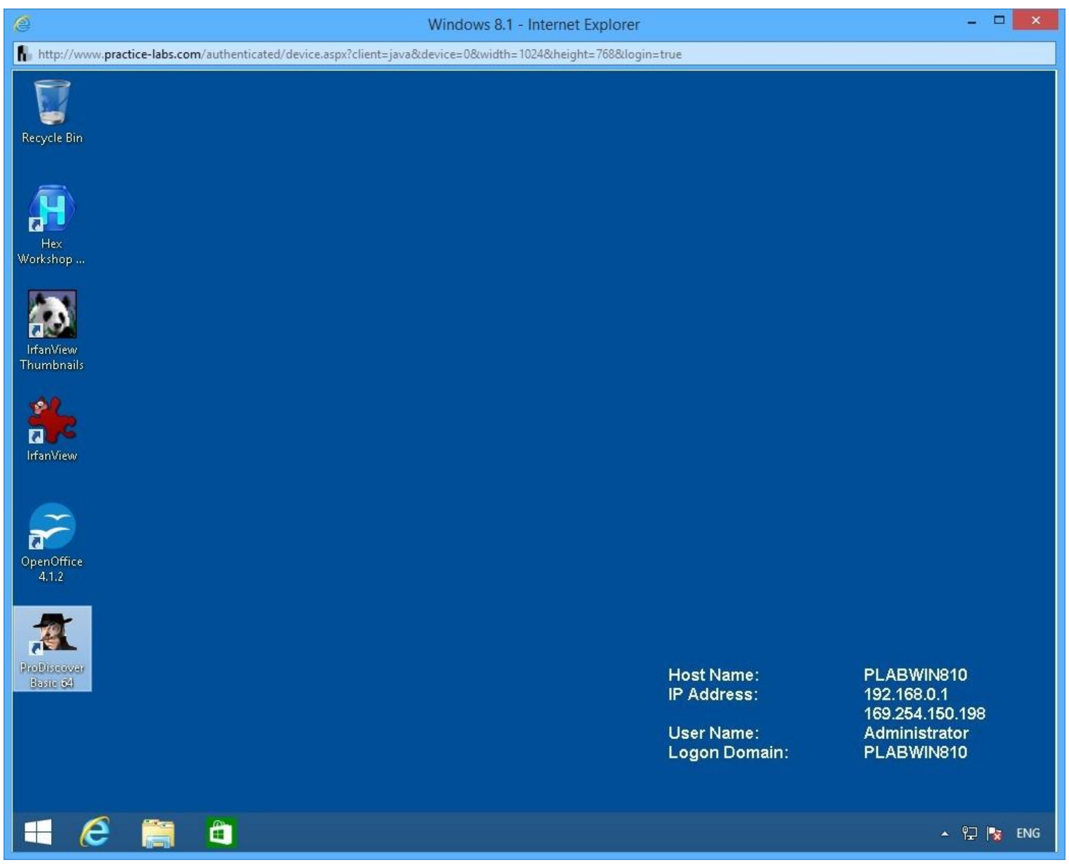
Để hiểu rõ hơn về công nghệ này, vui lòng tham khảo tài liệu khóa học của bạn hoặc sử dụng công cụ tìm kiếm ưa thích của bạn để nghiên cứu chủ đề chi tiết hơn. Hãy tham khảo giáo trình CHFI v9 hay tài liệu Computer Forensic tiếng Việt.

Nhiệm vụ 1 - Sử dụng ProDiscovery để phân tích bằng chứng

Trong các bước sau, bạn phân tích ổ đĩa của tổ chức George Montgomery. Nhiệm vụ đầu tiên là tải hình ảnh có được vào ProDiscover Basic bằng cách làm theo các bước sau:

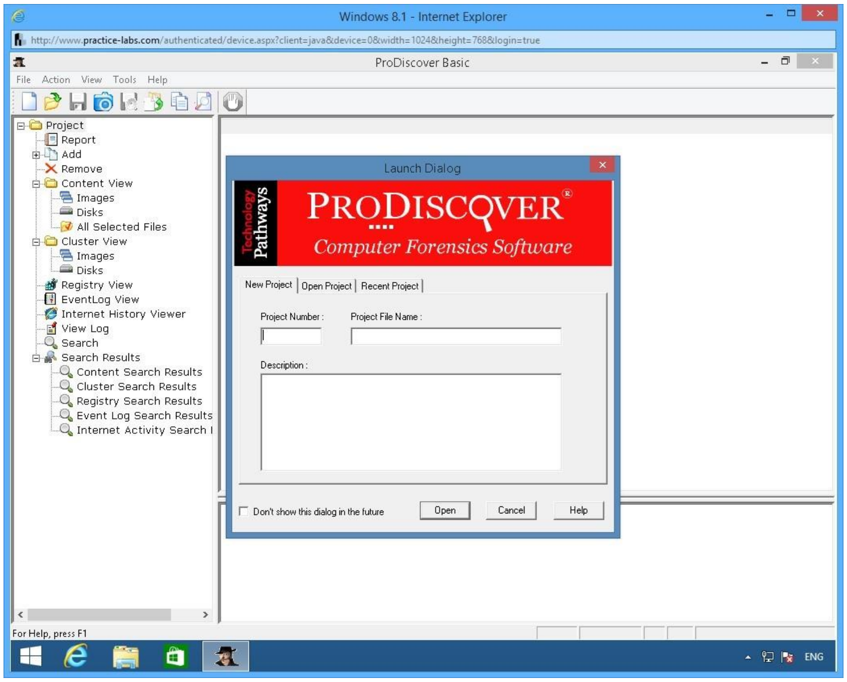
Bước 1

Trên thiết bị **PLABWIN810** , khởi động **ProDiscover Basic 64** như bạn đã làm trong hoạt động trước đó.



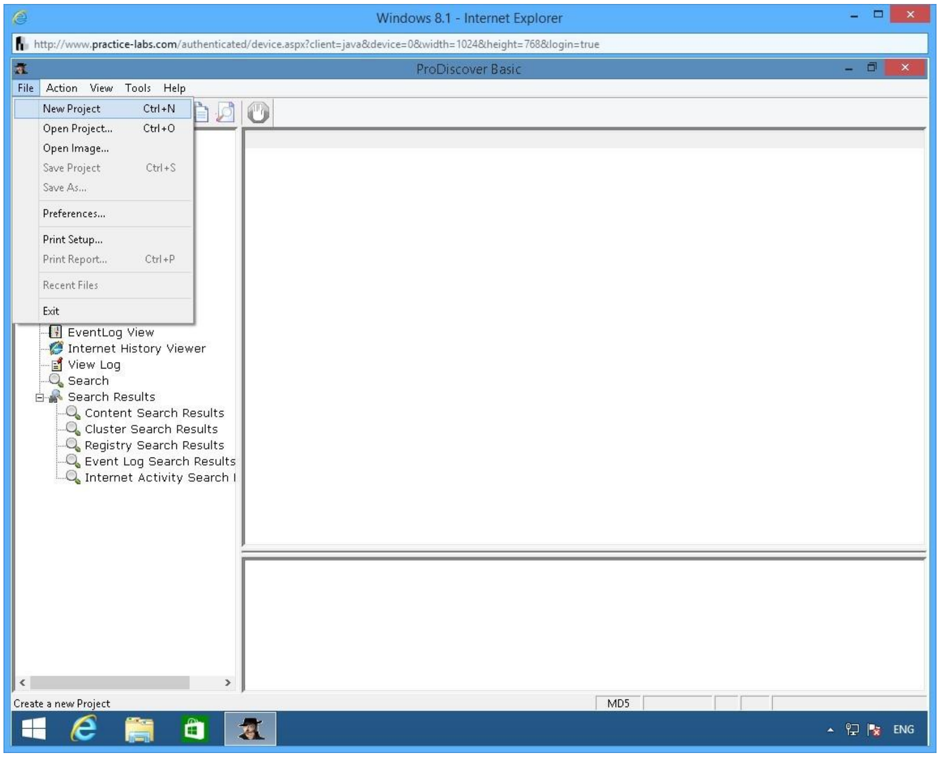
Bước 2

Nhấp vào **Hủy** trên hộp thoại Khởi chạy ProDiscover.



Bước 3

Để tạo một trường hợp hay tình huống mới, hãy nhấp vào **Tệp** , **Dự án Mới** từ menu.

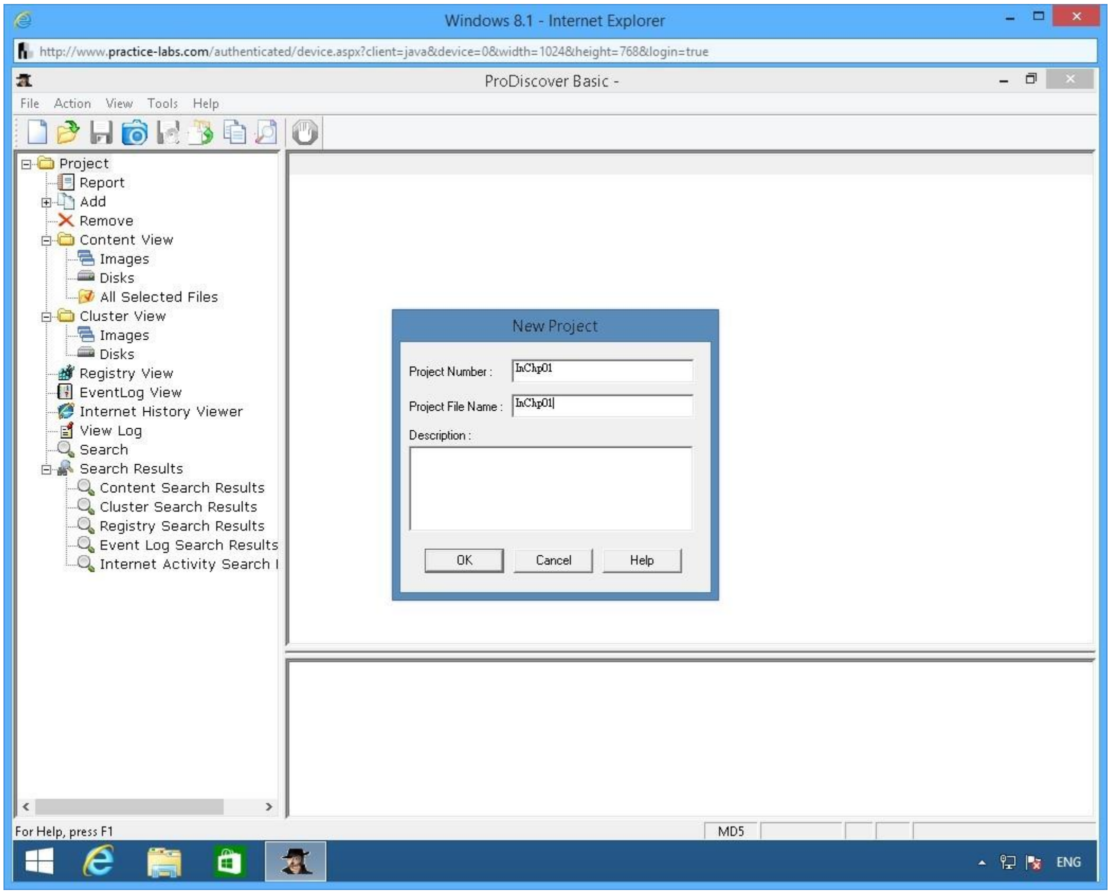


Bước 4

Trong hộp thoại **Dự án mới** , trong hộp văn bản **Số dự án** và một lần nữa trong hộp văn bản **Tên tệp dự án** , hãy nhập:

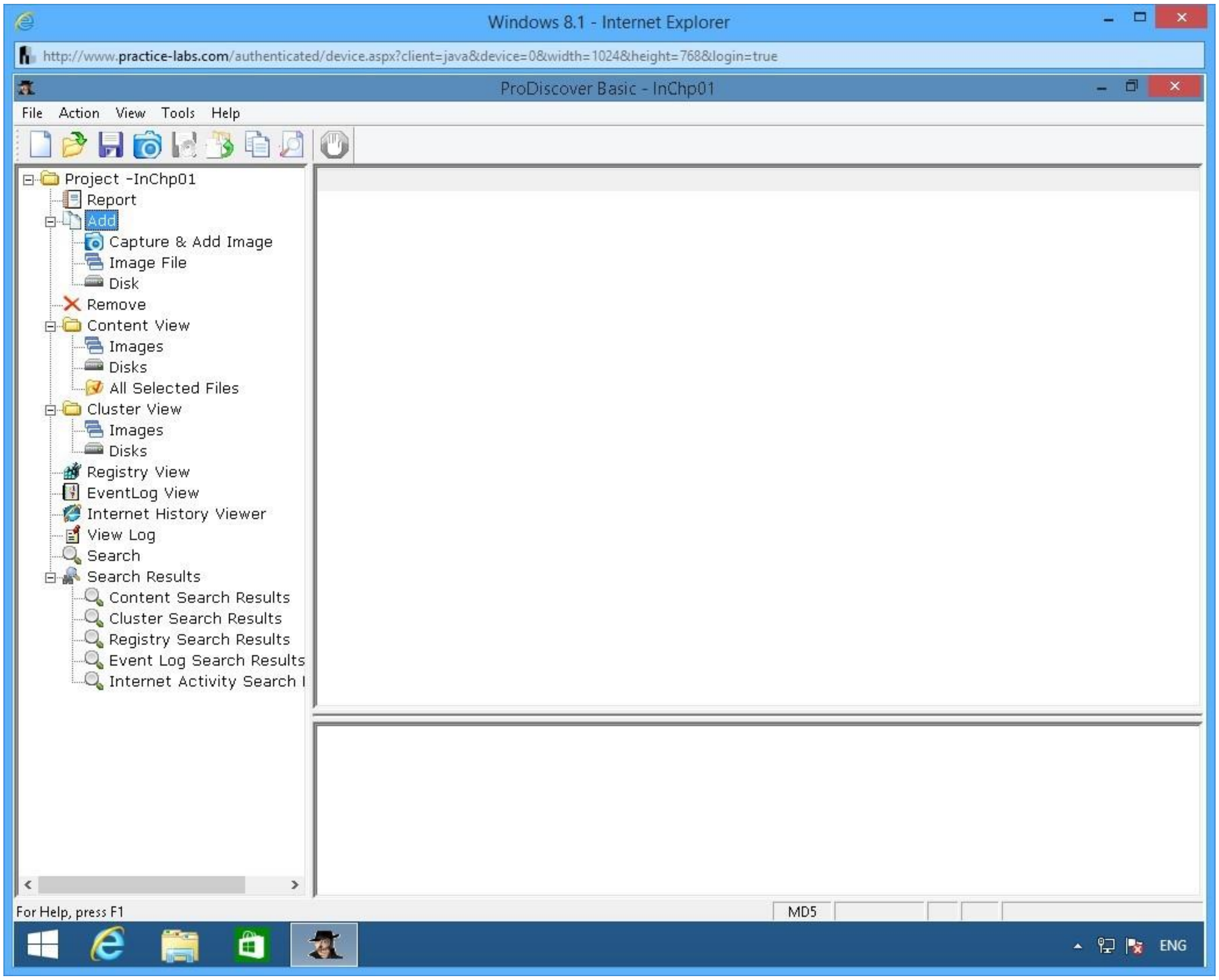
```
InChp01
```

Bấm **OK** .



Bước 5

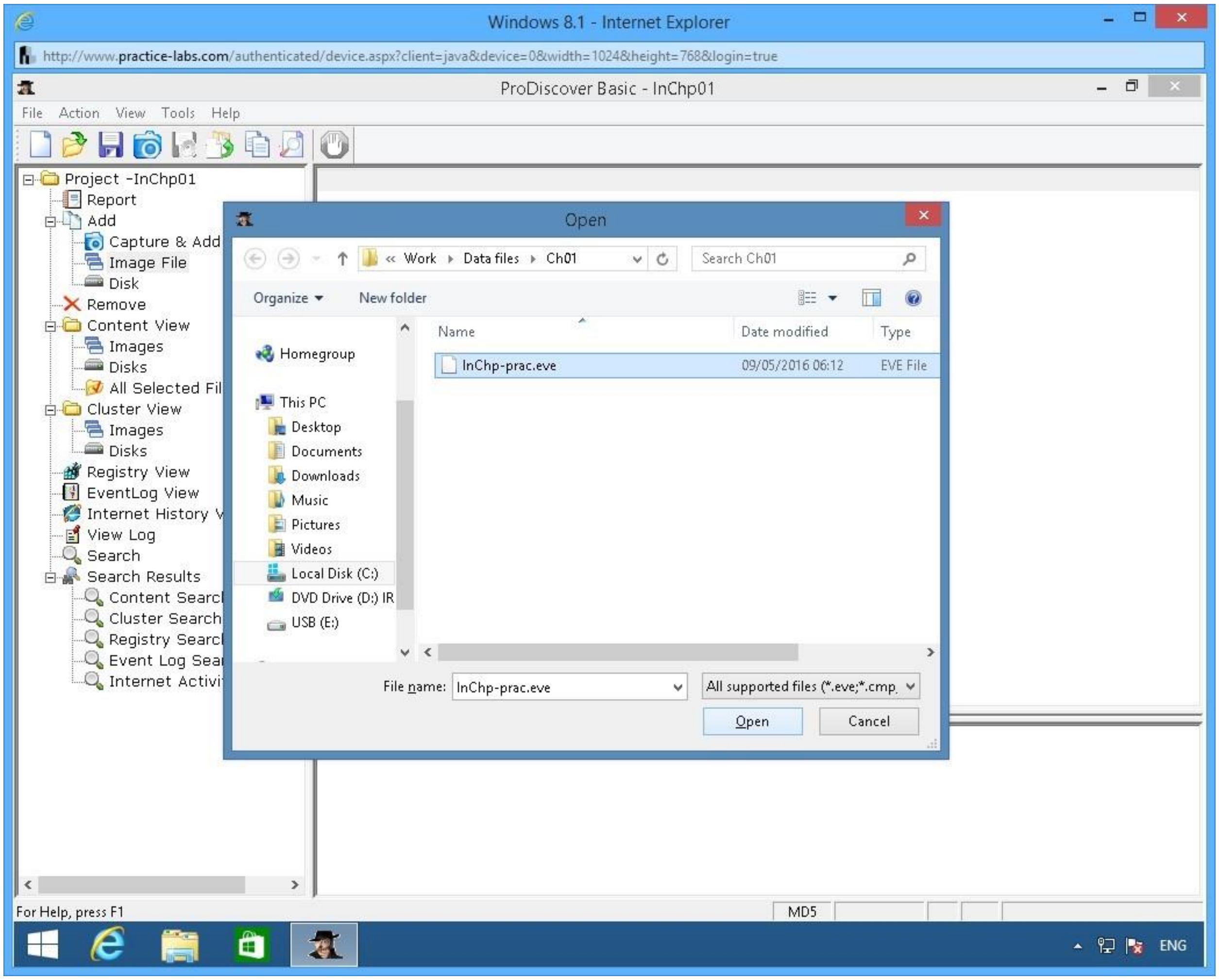
Trong chế độ xem dạng cây của cửa sổ chính, bấm để Mở rộng mục **Thêm** (Add), rồi bấm **Tệp Hình ảnh** (Image File)



Bước 6

Trong hộp thoại **Open** , bạn sẽ được chuyển hướng đến thư mục **c: \ Work> Data files> Ch01** chứa hình ảnh, nhấp vào **tệp InChp01-Practice.eve** .

Nhấp vào **Open** .



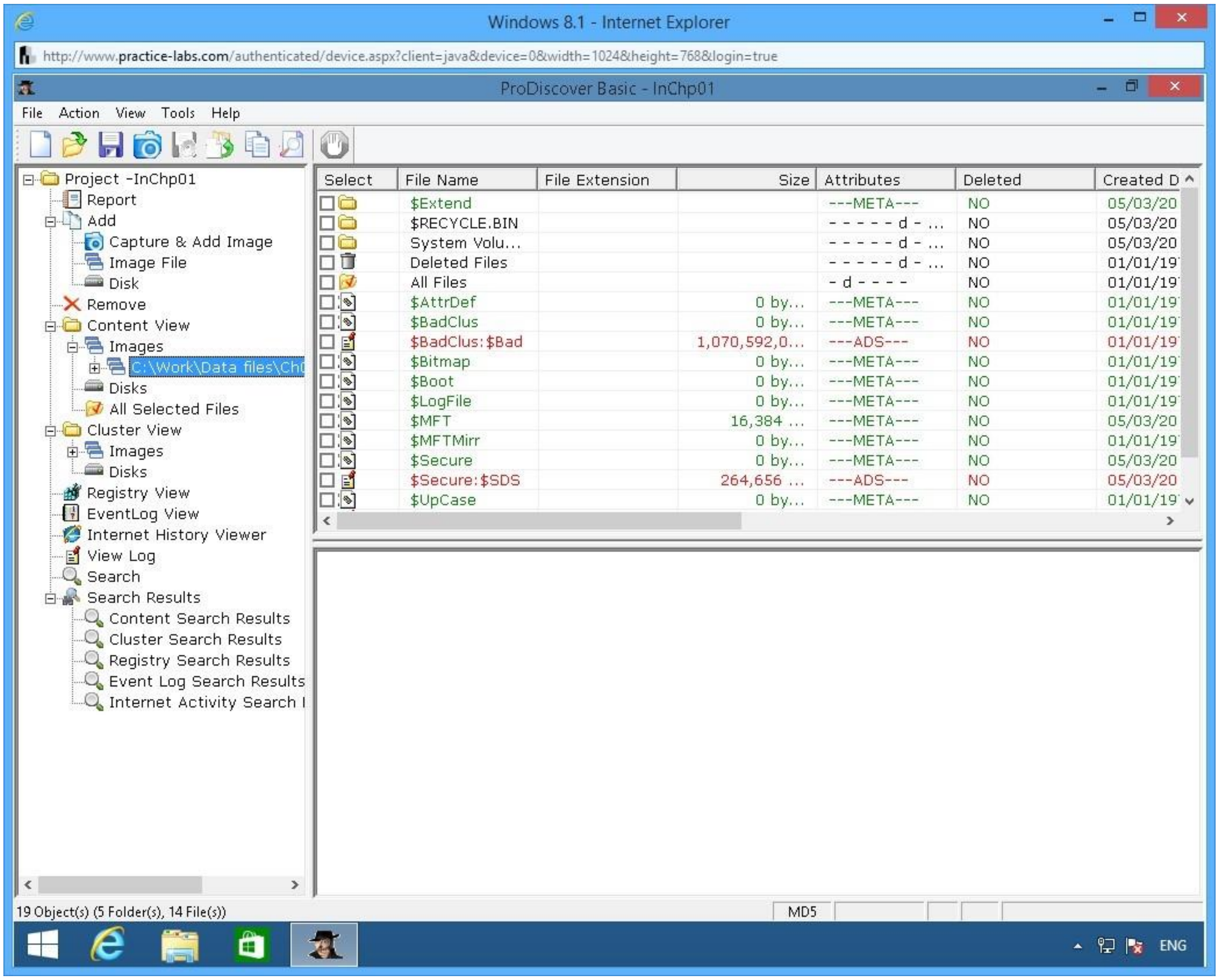
Bước 7

Bấm **Có** trong hộp thông báo Tự động Kiểm tra Hình ảnh, nếu cần.

Nhiệm vụ tiếp theo là hiển thị nội dung của dữ liệu thu được.

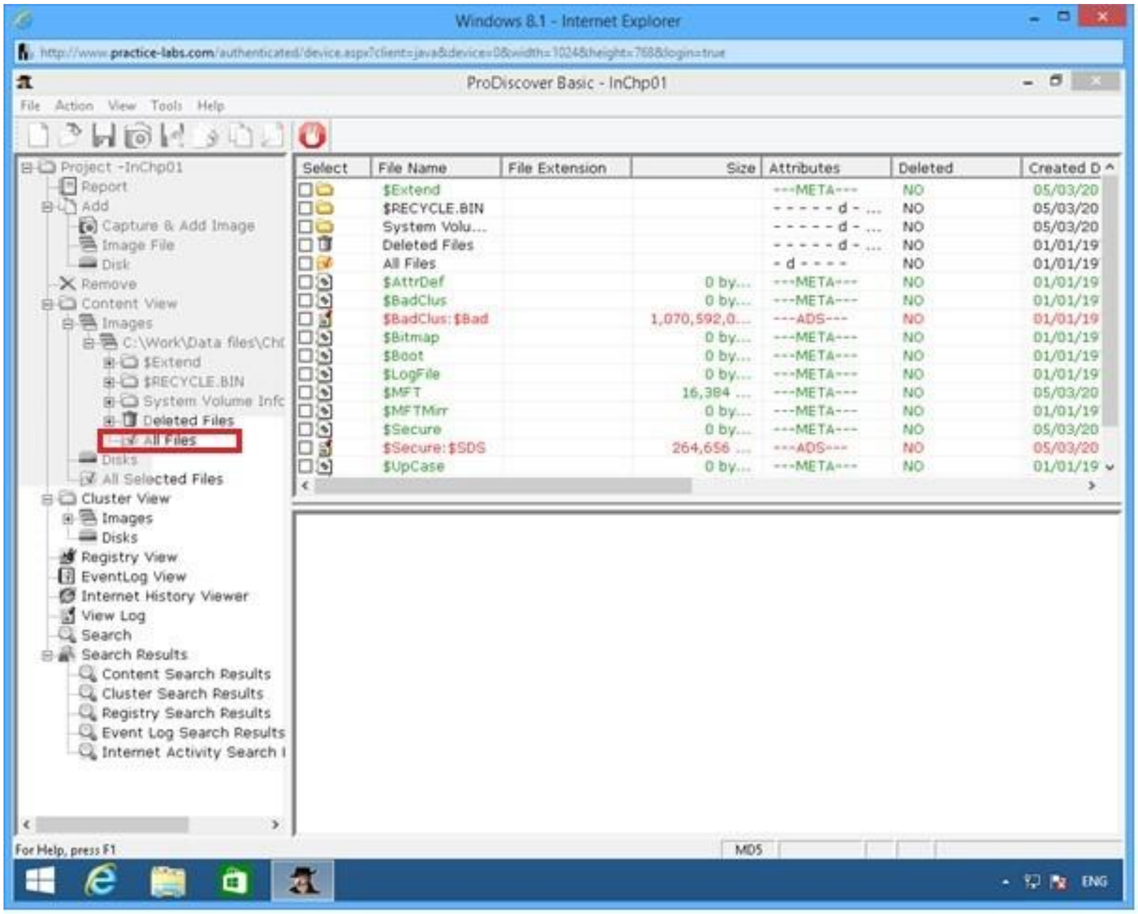
Trong chế độ xem dạng cây, hãy nhấp để Mở rộng **Chế độ xem nội dung** , nếu cần.

Nhấp để Mở rộng **Hình ảnh** và nhấp vào đường dẫn tên tệp hình ảnh **C: \ Work \ Chap01 \ Chapter \ InChp01-doing.eve** .



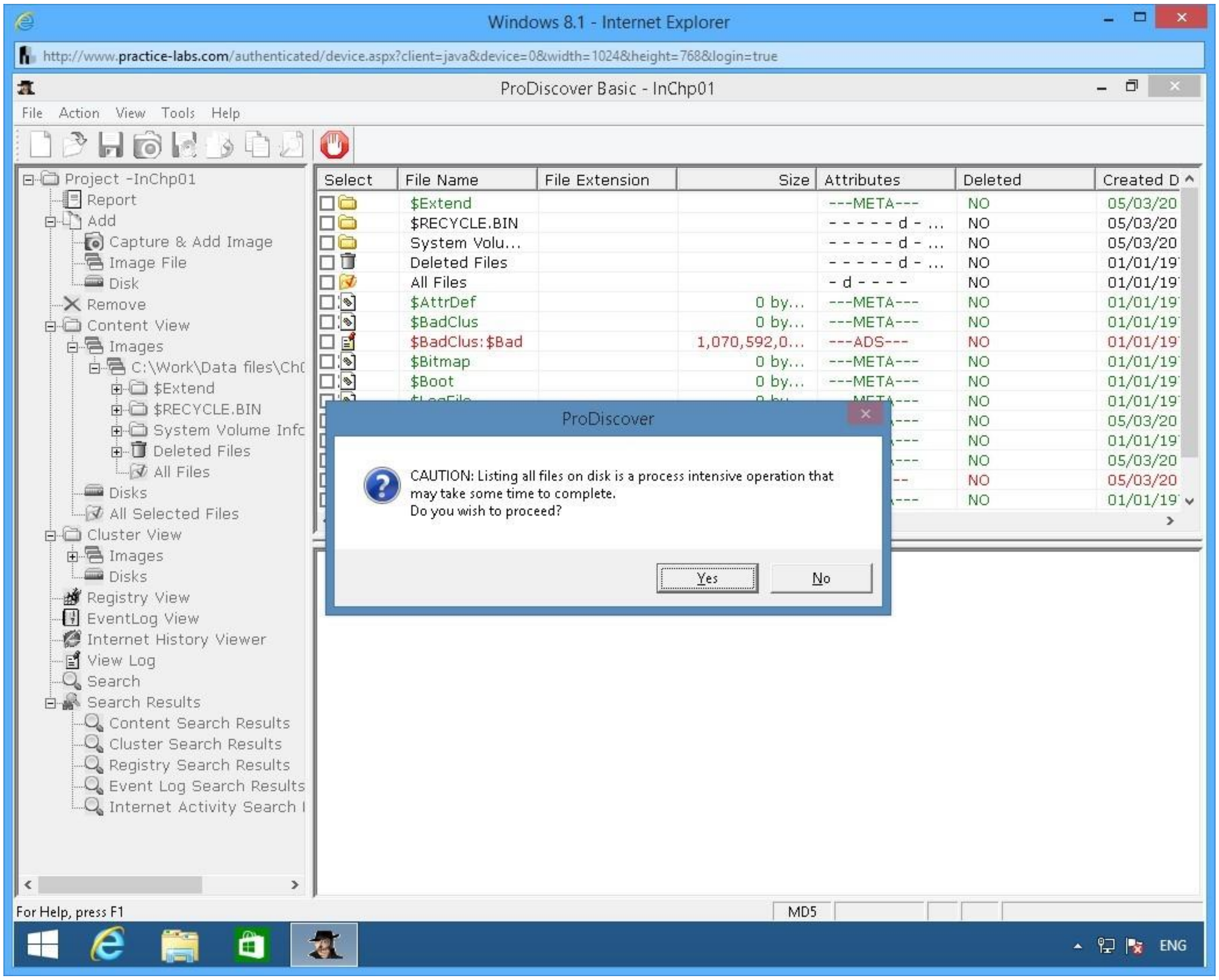
Bước 8

Tiếp theo, bấm vào dấu **+** ở phía trước tên đường dẫn tệp hình ảnh, sau đó bấm **Tất cả các tệp** bên dưới đường dẫn tên tệp hình ảnh.



Bước 9

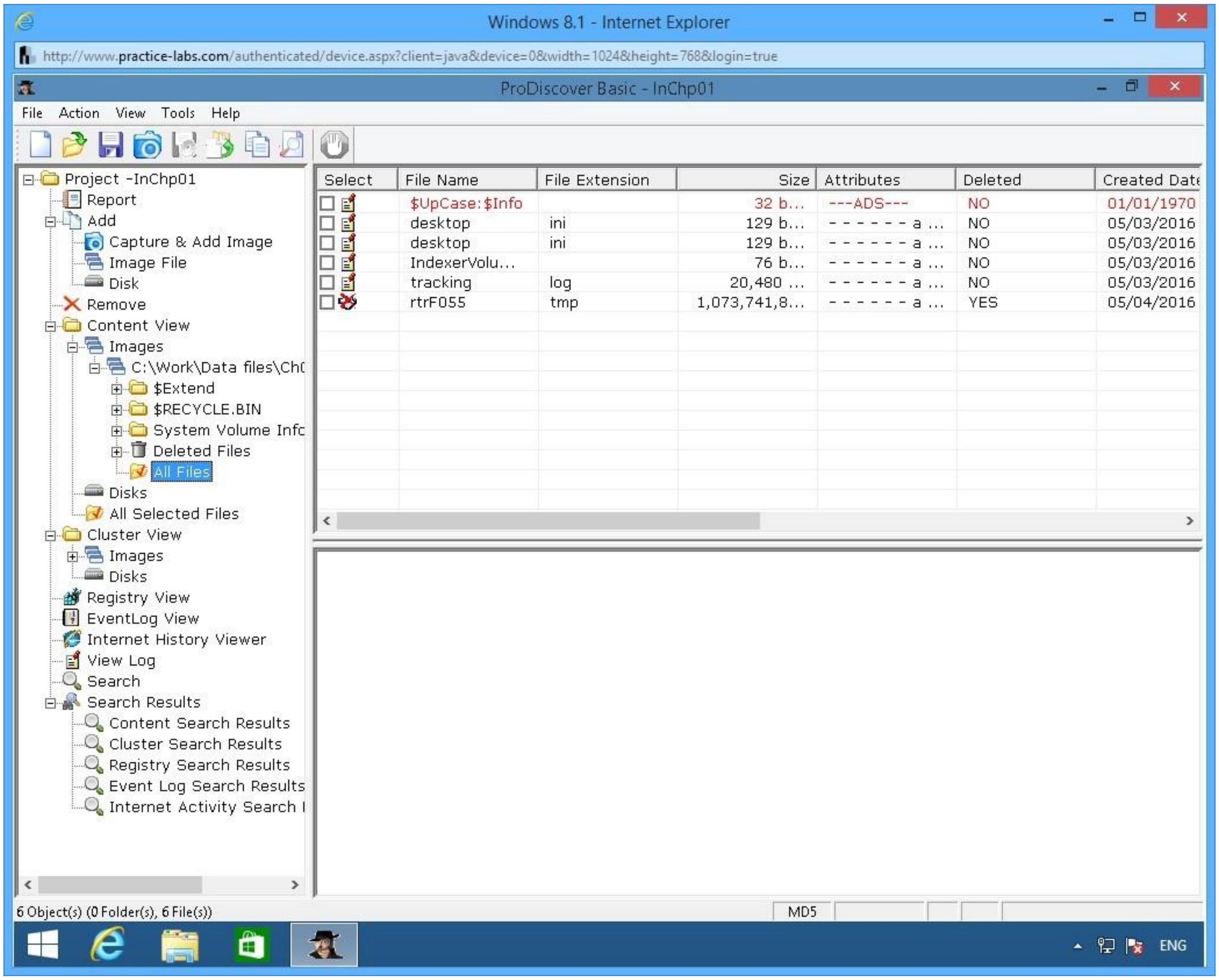
Khi hộp thoại **ProDiscover - CAUTION** Open ra, hãy bấm **Có** .



Bước 10

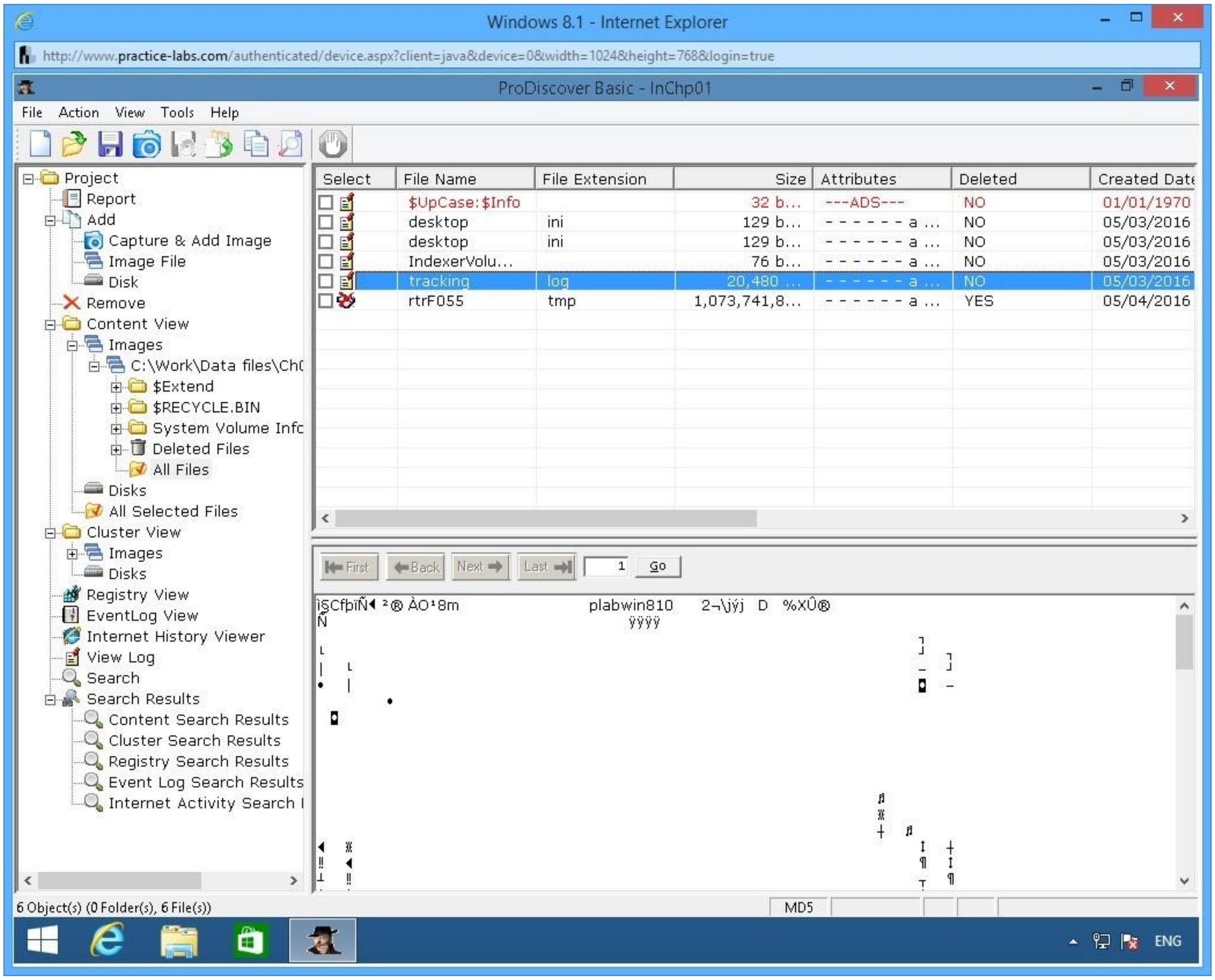
Sau đó, **tệp InChp01-doing.eve** được tải trong cửa sổ chính.

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Bước 11

Trong ngăn phía trên bên phải (vùng làm việc), bấm vào tệp **tracking.log** để xem nội dung của nó trong vùng dữ liệu.

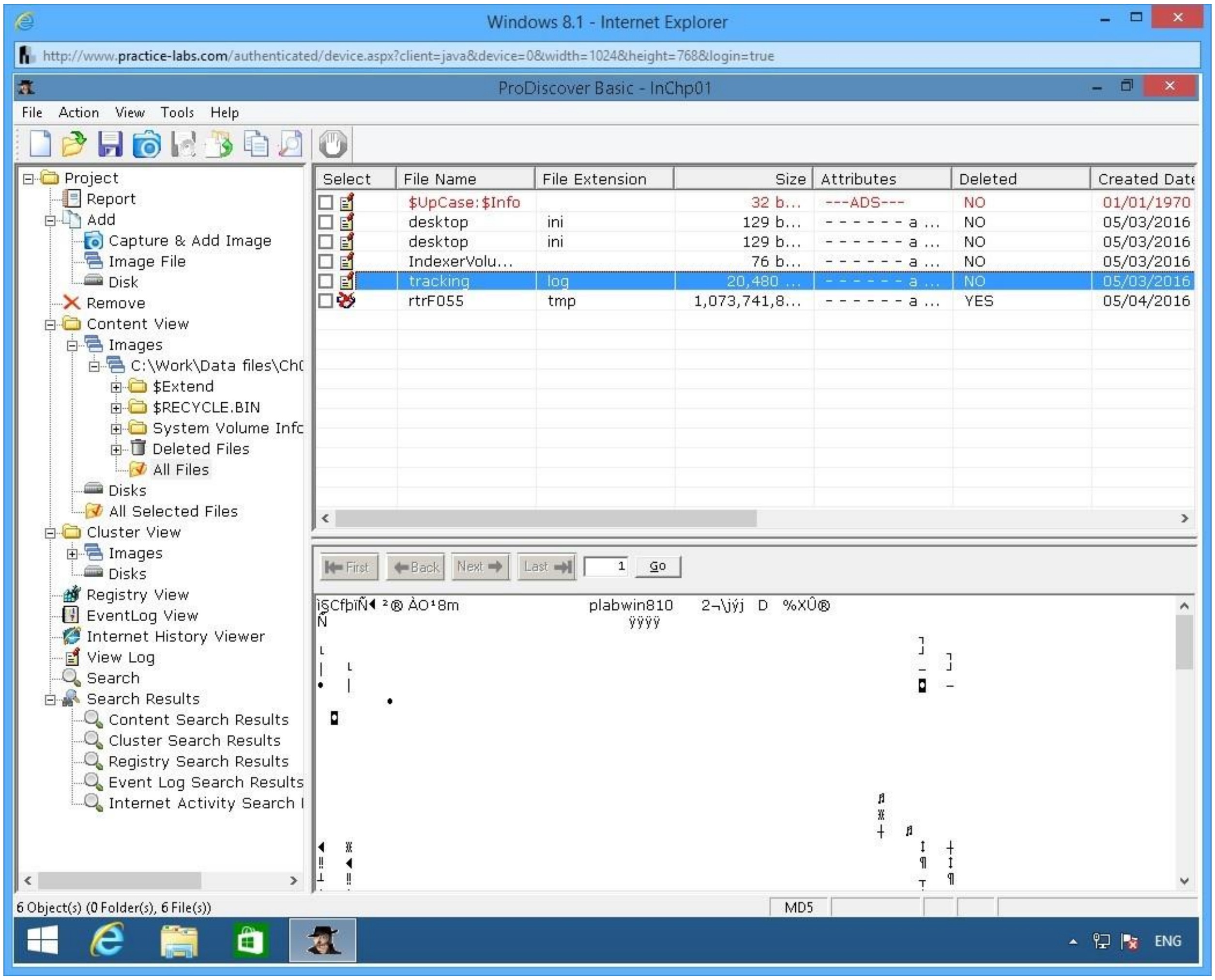


Bước 12

Trong vùng dữ liệu, bạn sẽ thấy nội dung của tệp **tracking.log** . Tiếp tục điều hướng qua các khu vực làm việc và dữ liệu và kiểm tra nội dung của bằng chứng đã thu hồi.

Để ProDiscover Basic chạy cho hoạt động tiếp theo.

Giữ cửa sổ **ProDiscover Basic - InChp01** Open.



Giữ cho thiết bị được bật nguồn ở trạng thái hiện tại và tiến hành tác vụ tiếp theo.

Nhiệm vụ 2 - Phân tích dữ liệu

Bước tiếp theo là phân tích dữ liệu và tìm kiếm thông tin liên quan đến khiếu nại. *Phân tích dữ liệu có thể là công việc tốn nhiều thời gian nhất,* ngay cả khi bạn biết chính xác những gì cần tìm trong bằng chứng. Phương pháp để xác định vị trí bằng chứng là tìm kiếm các giá trị dữ liệu cụ thể đã biết. Giá trị dữ liệu có thể là các từ duy nhất hoặc các ký tự không in được, chẳng hạn như mã thập lục phân. Ngoài ra còn có các mã ký tự có thể in được không thể tạo từ bàn phím, chẳng hạn như các ký hiệu bản quyền ([a]) hoặc nhãn hiệu đã đăng ký (TM). Nhiều chương trình pháp y kỹ thuật số có thể tìm kiếm các chuỗi ký tự (chữ cái và số) và các giá trị thập lục phân, chẳng hạn như A9 cho biểu tượng bản quyền hoặc AE cho biểu tượng nhãn hiệu đã đăng ký. Tất cả các giá trị dữ liệu có thể tìm kiếm này được gọi là "từ khóa". Với ProDiscover Basic, bạn có thể tìm kiếm các từ khóa quan tâm trong trường hợp hay tình huống cần xử lý (các ứng dụng pháp y số thường gọi là Case hay cũng có thể là vụ án).

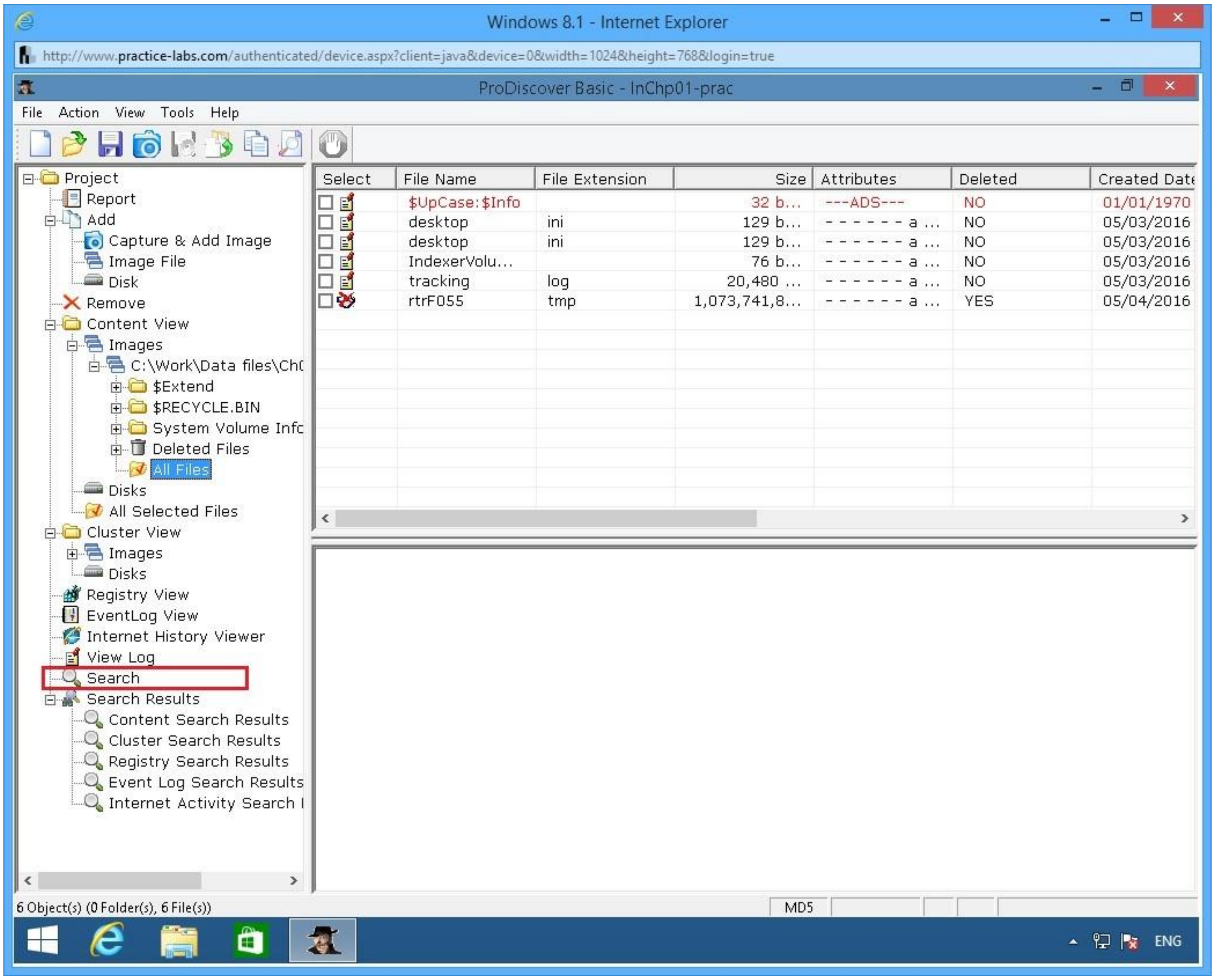
Bước 1

Trên thiết bị **PLABWIN810** , cửa sổ **ProDiscover Basic - InChp-01** đang Open.

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo

Đảm bảo rằng **Chế độ xem nội dung> Hình ảnh> C: \ Work \ Data files \ Ch01 \ Inchp-Practice.eve** sau đó nút **Tất cả tệp** được chọn.

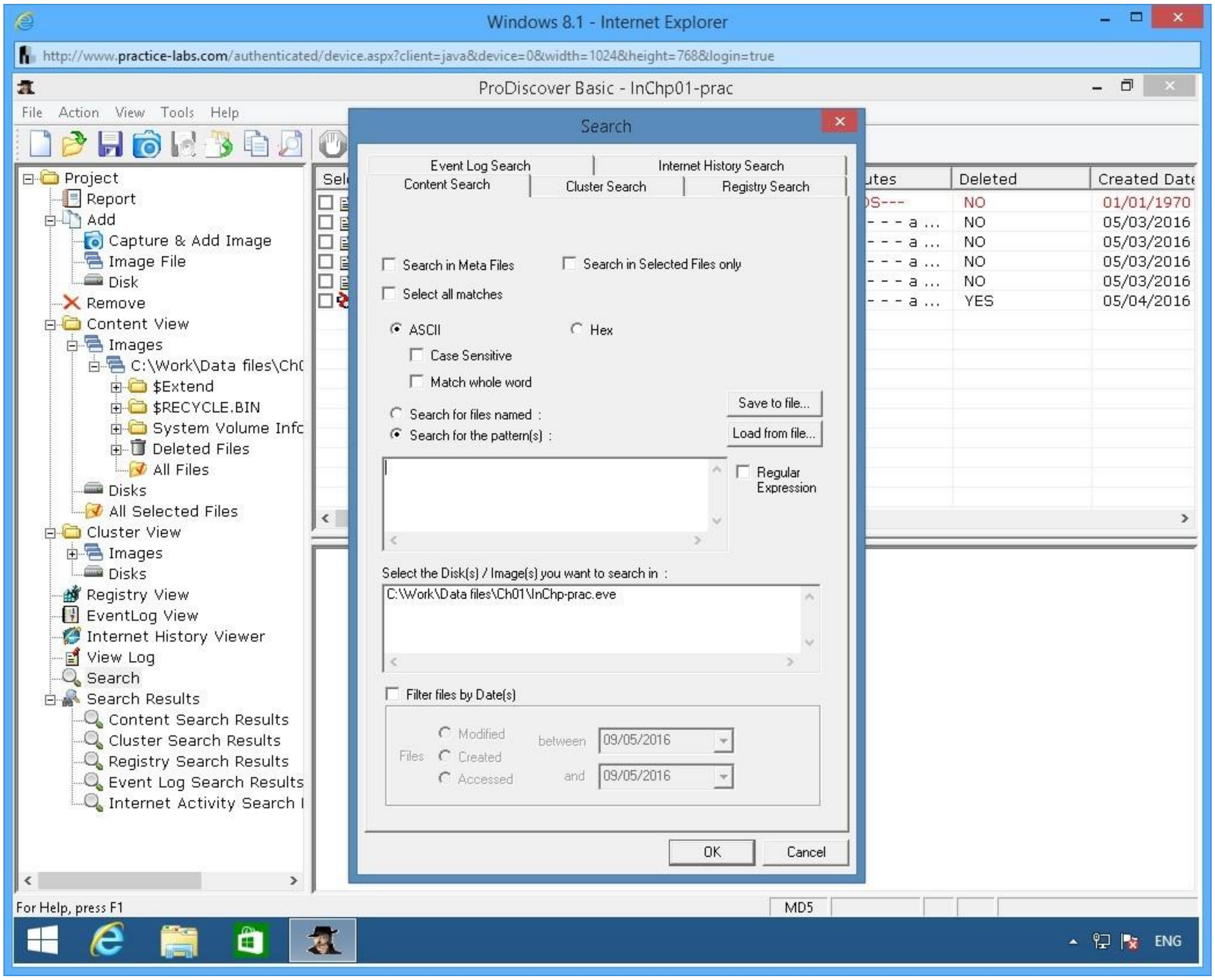
Trong chế độ xem dạng cây, hãy nhấp vào **Tìm kiếm** (Search).



Bước 2

Trong hộp thoại **Tìm kiếm** , bấm vào tab **Tìm kiếm nội dung** , nếu cần.

Bấm vào hộp kiểm **Chọn tất cả các kết quả phù hợp** , nút tùy chọn **ASCII và** nút tùy chọn **Tìm kiếm (các) mẫu** , nếu chúng chưa được chọn.



Bước 3

Tiếp theo, trong hộp văn bản bên dưới nút tùy chọn **Tìm kiếm (các) mẫu** , hãy nhập:

```
plabwin810
```

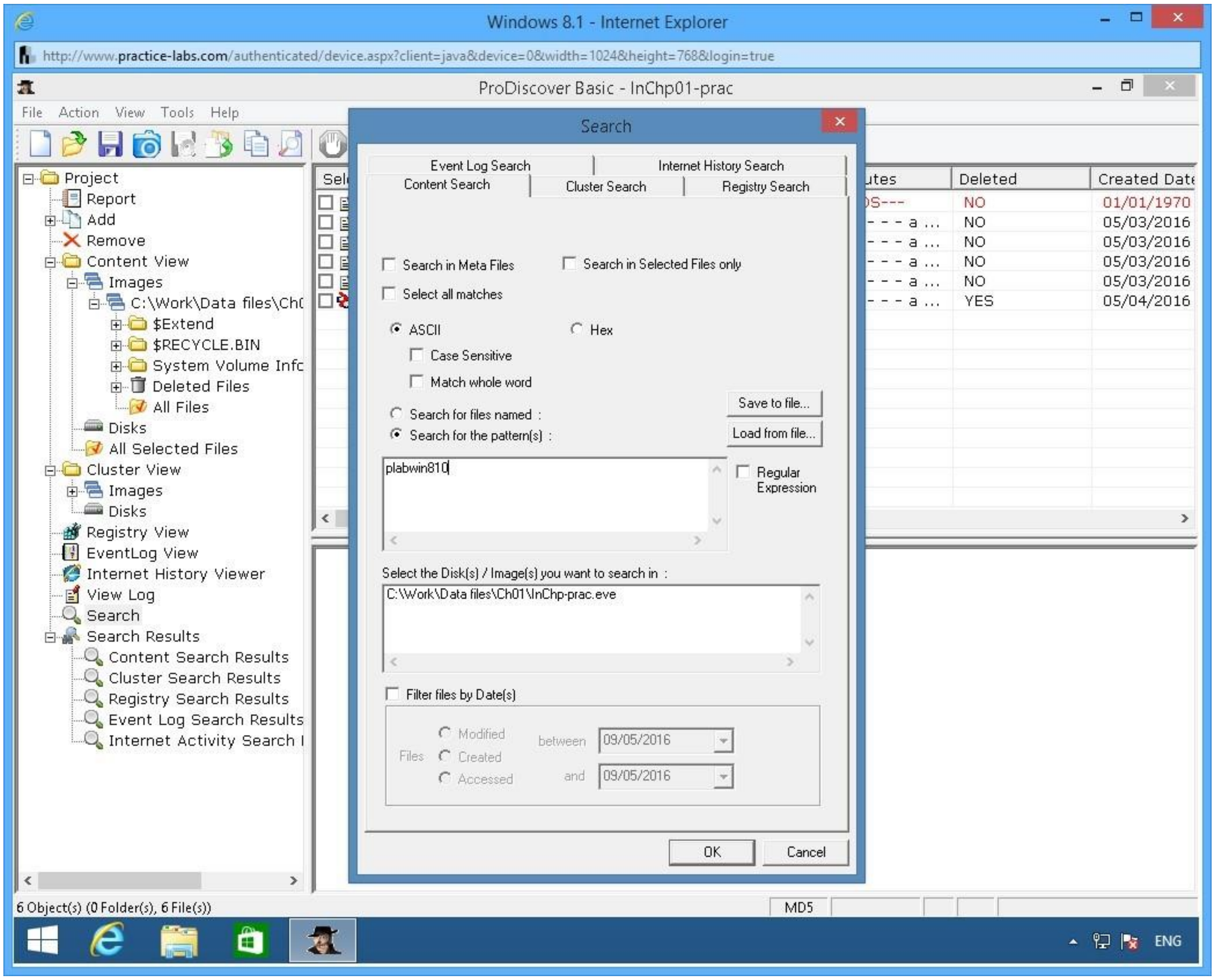
Lưu ý *: Bạn có thể liệt kê các từ khóa riêng biệt hoặc kết hợp các từ với các toán tử logic*

Boolean AND, OR và NOT. Tìm kiếm một từ khóa phổ biến tạo ra quá nhiều lượt truy cập và

khiến việc tìm kiếm bằng chứng quan tâm đến trường hợp trở nên khó khăn. Áp dụng logic

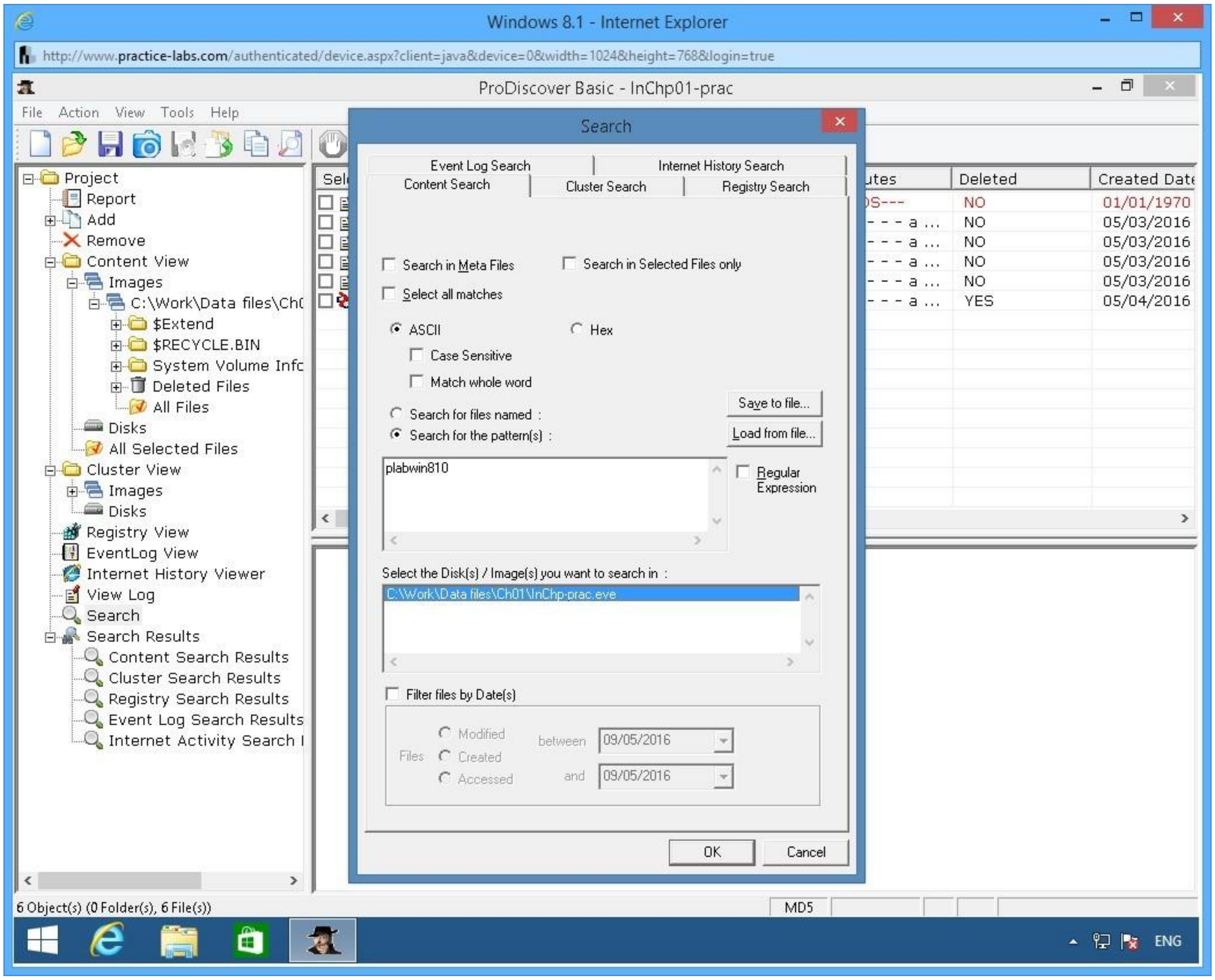
Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo

Boolean có thể giúp giảm số lần truy cập quá mức không liên quan, được gọi là "lần truy cập dương tính giả.



Bước 4

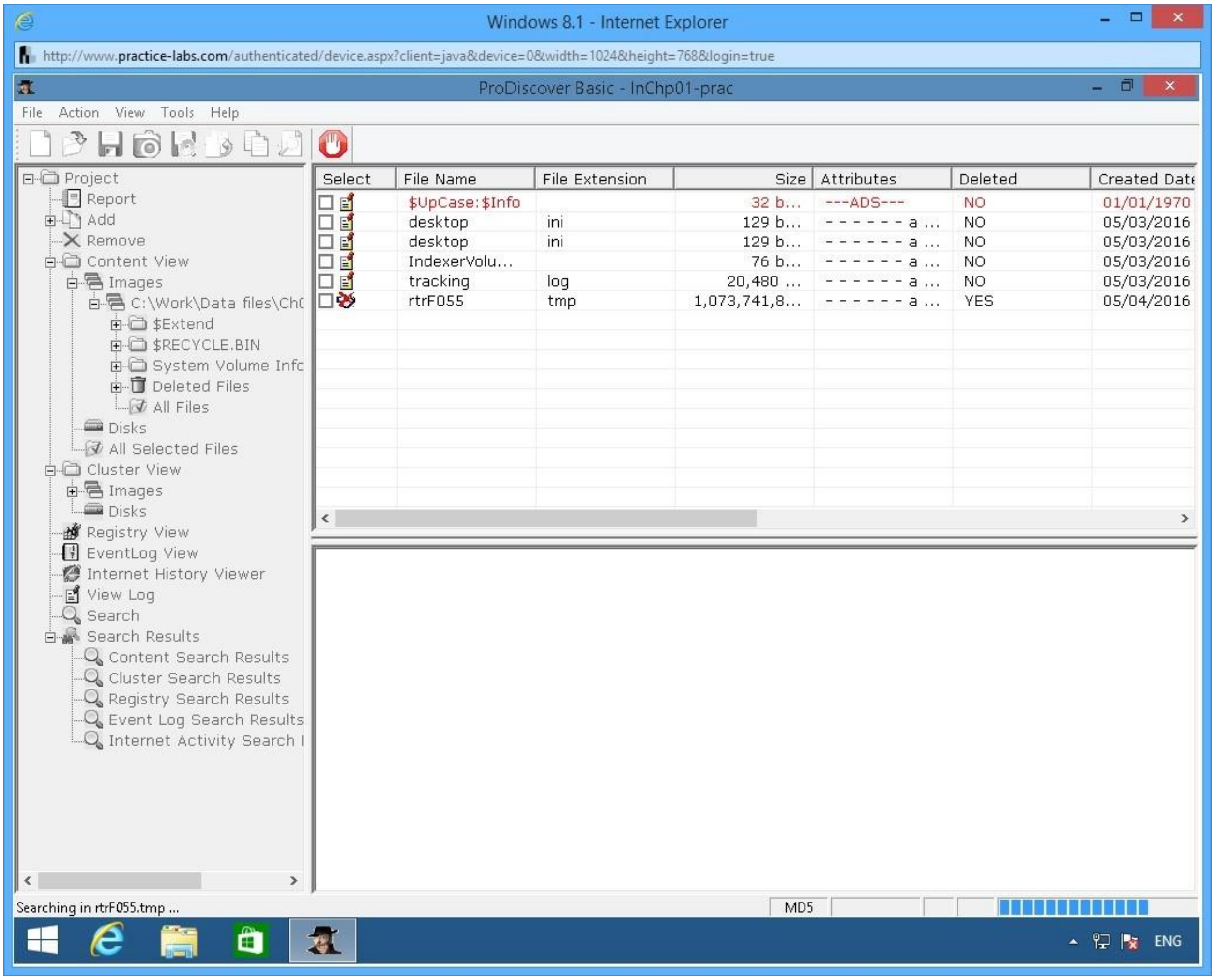
Bên dưới **Chọn (các) Đĩa / (các) Hình ảnh bạn muốn tìm kiếm trong** phần, hãy bấm **C: \ Work \ Chap01 \ Chương \ InChp01-practice.eve** (thay thế đường dẫn đến thư mục công việc của bạn), rồi bấm **OK** để bắt đầu Tìm kiếm.



Bước 5

Vui lòng đợi trong khi **ProDiscover Basic** chạy tìm kiếm.

Quá trình này sẽ mất vài giây.

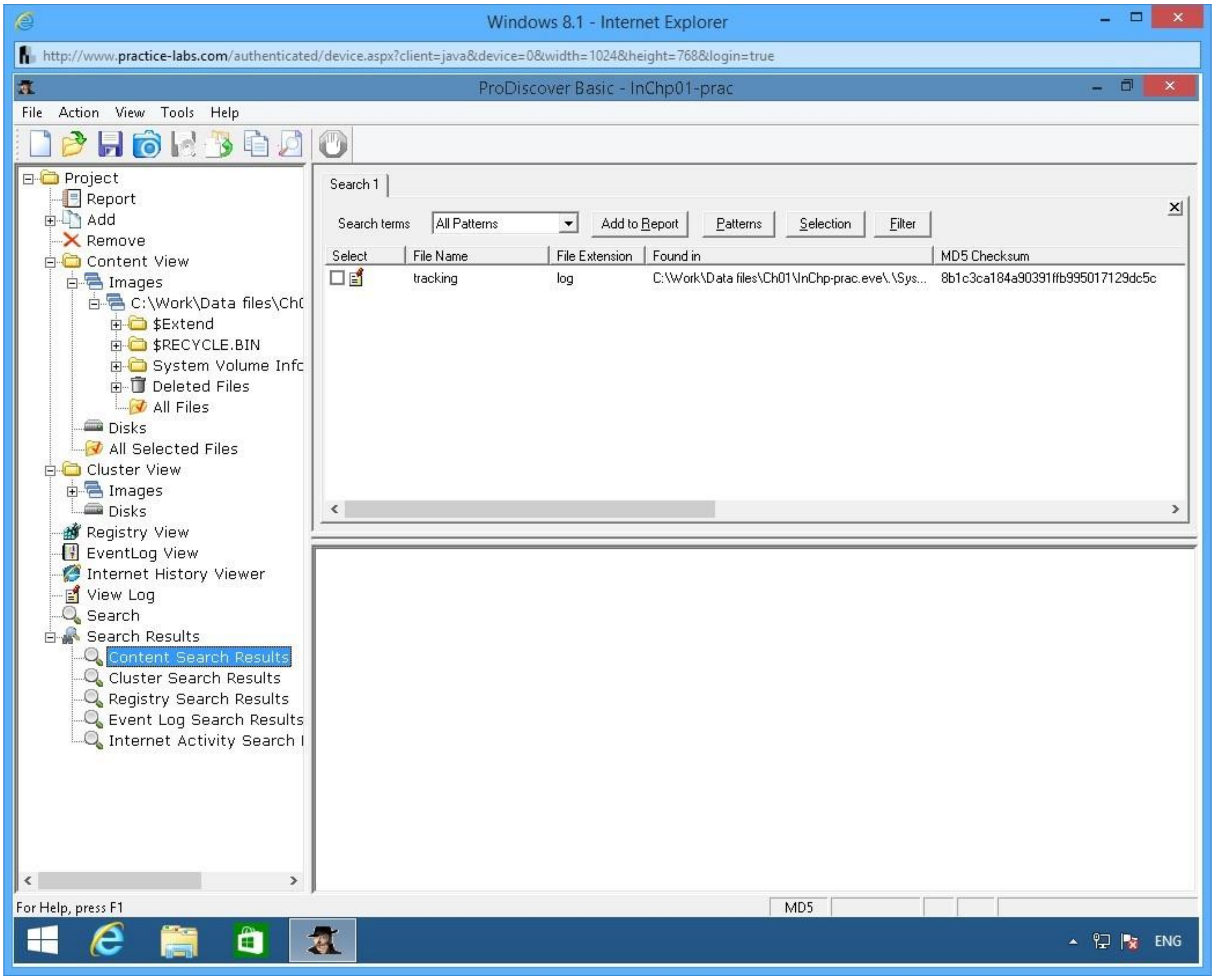


Bước 6

Khi kết thúc tìm kiếm, ProDiscover hiển thị kết quả trong ngăn kết quả tìm kiếm trong vùng làm việc. Lưu ý các tab có nhãn **Tìm kiếm 1** .

Đối với mỗi tìm kiếm bạn thực hiện trong một trường hợp, ProDiscover thêm một tab mới để giúp lập danh mục các tìm kiếm của bạn.

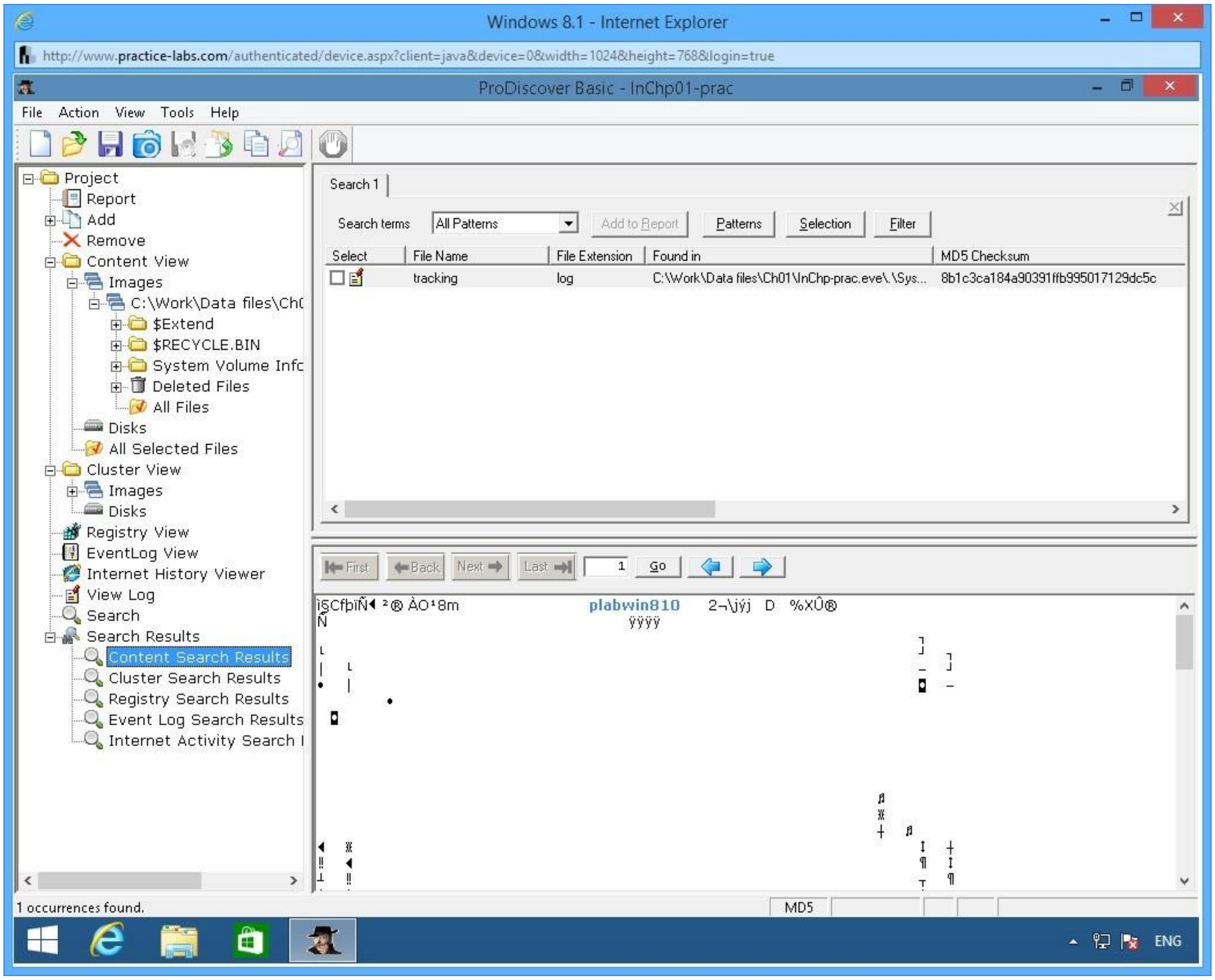
Lưu ý rằng tệp tracking.log được tìm thấy chứa chuỗi ' **plabwin810** .'



Bước 7

Nhấp vào nút **Kết quả Tìm kiếm Nội dung** (Content Search Result) trong ngăn kết quả tìm kiếm và kiểm tra nội dung của nó trong vùng dữ liệu.

Giữ cửa sổ **ProDiscover Basic luôn** Open.



Giữ cho thiết bị được bật nguồn ở trạng thái hiện tại và tiến hành tác vụ tiếp theo.

Nhiệm vụ 3 - Tạo Report

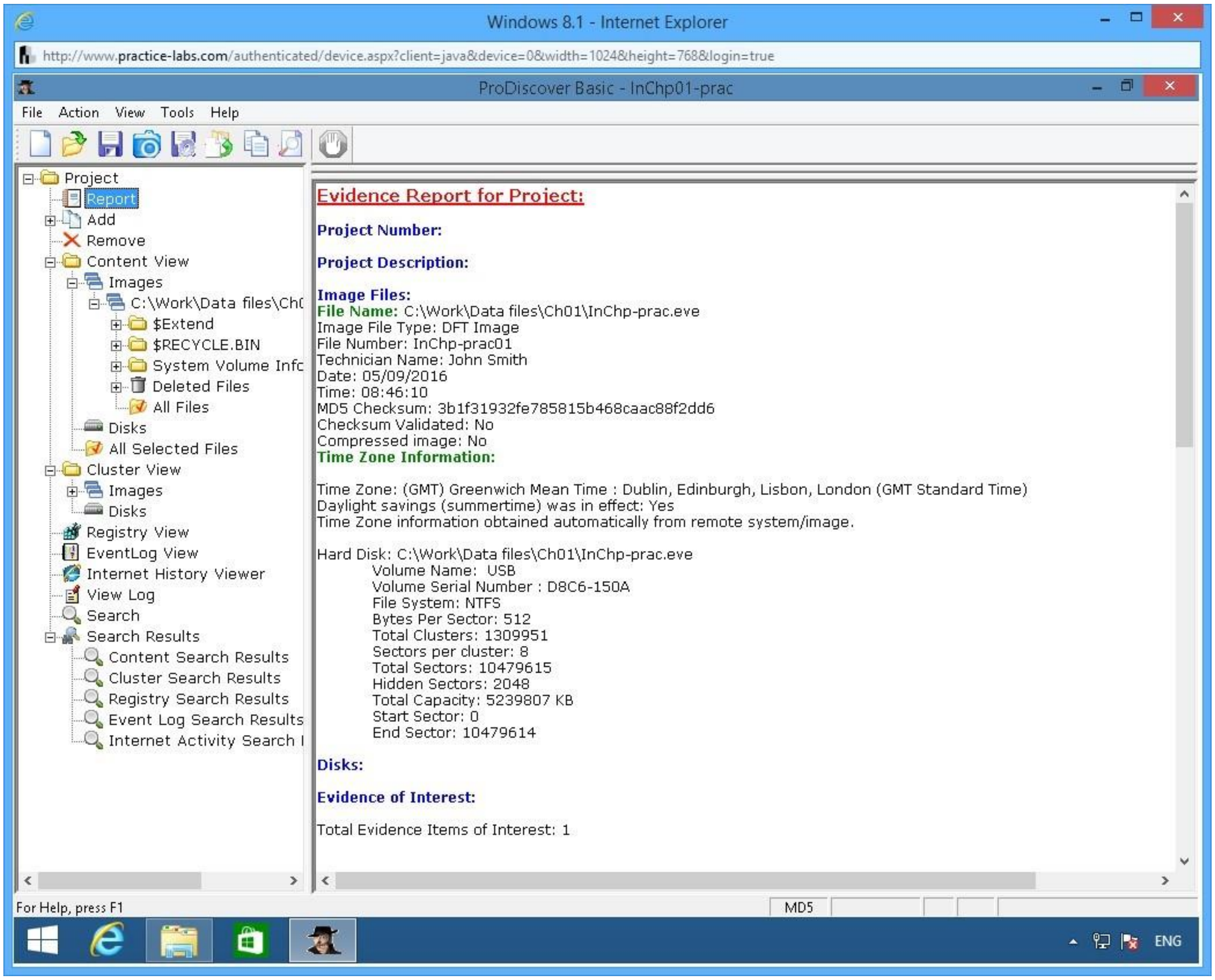
Bạn cũng có thể chọn các mục cụ thể và thêm chúng vào Report. Ví dụ: để chọn tệp trong vùng làm việc, hãy bấm vào hộp kiểm trong cột Chọn bên cạnh tệp để Open hộp thoại Thêm nhận xét. Nhập mô tả và bấm OK. Nhận xét mô tả sau đó được thêm vào Report ProDiscover Basic.

Để tạo Report trong ProDiscover Basic, hãy thực hiện các bước sau:

Bước 1

Trên thiết bị **PLABWIN810** , cửa sổ **ProDiscover Basic - InChp01-Practice** đang Open.

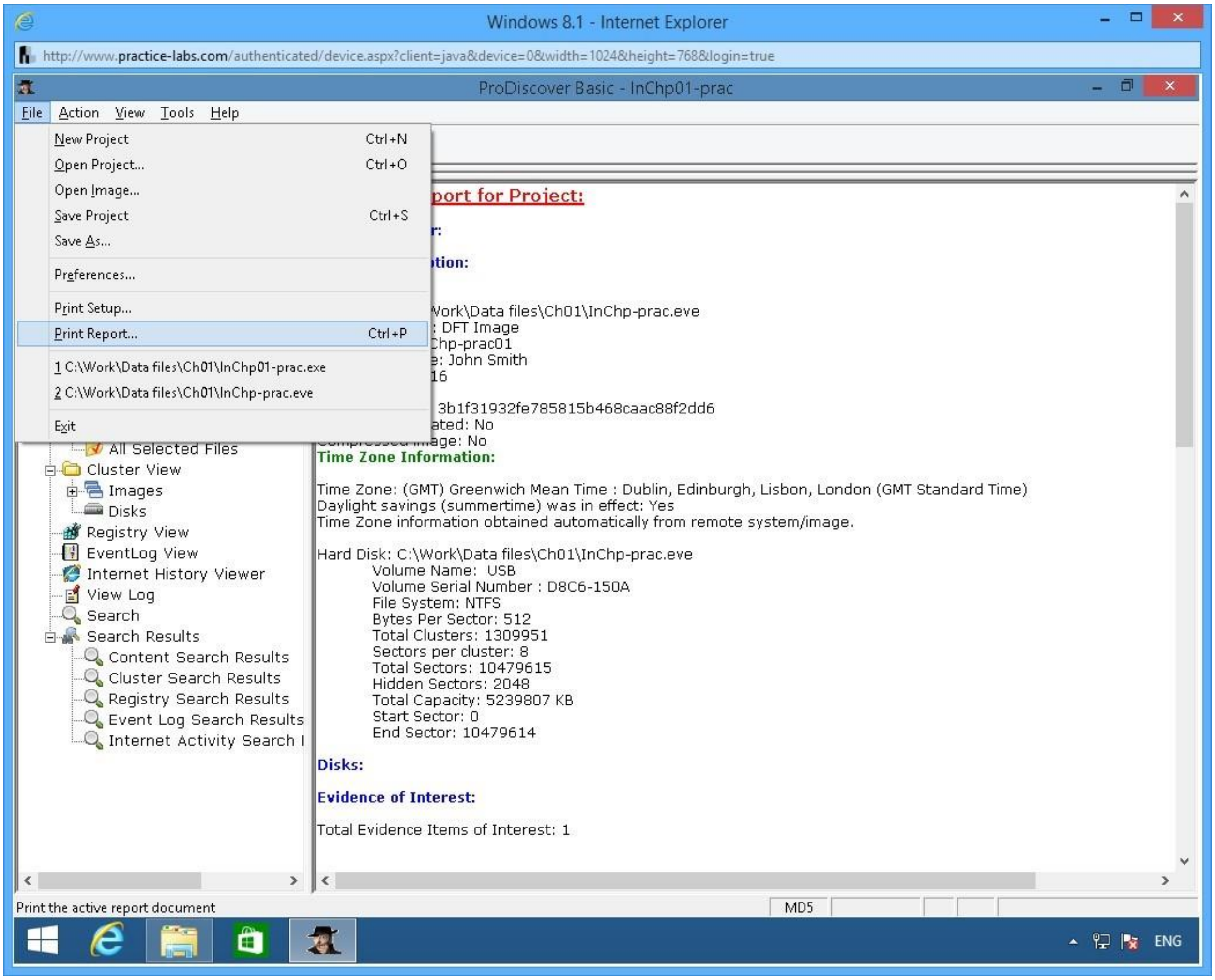
Trong chế độ xem dạng cây, hãy nhấp vào **Report** (Report). Sau đó, Report được hiển thị trong ngăn bên phải.



Bước 2

Để in Report, hãy nhấp vào **Tệp** (File), **In Report** (Print Report) từ menu.

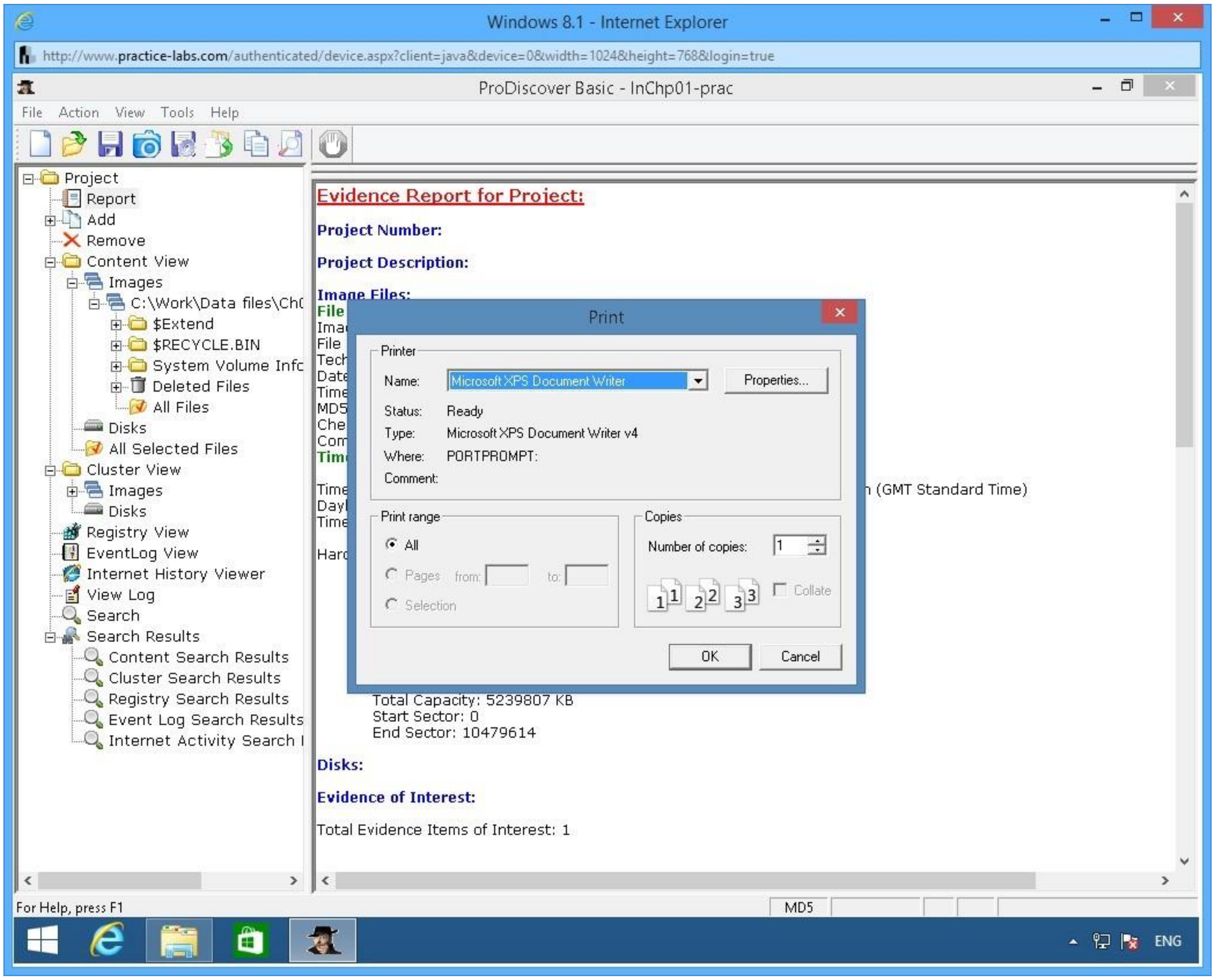
Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Bước 3

Vì không có máy in vật lý nào được cài đặt trên thiết bị phòng thí nghiệm, bạn sẽ chọn in Report bằng Microsoft XPS Document Writer.

Trong hộp thoại **In** , bấm **OK** .

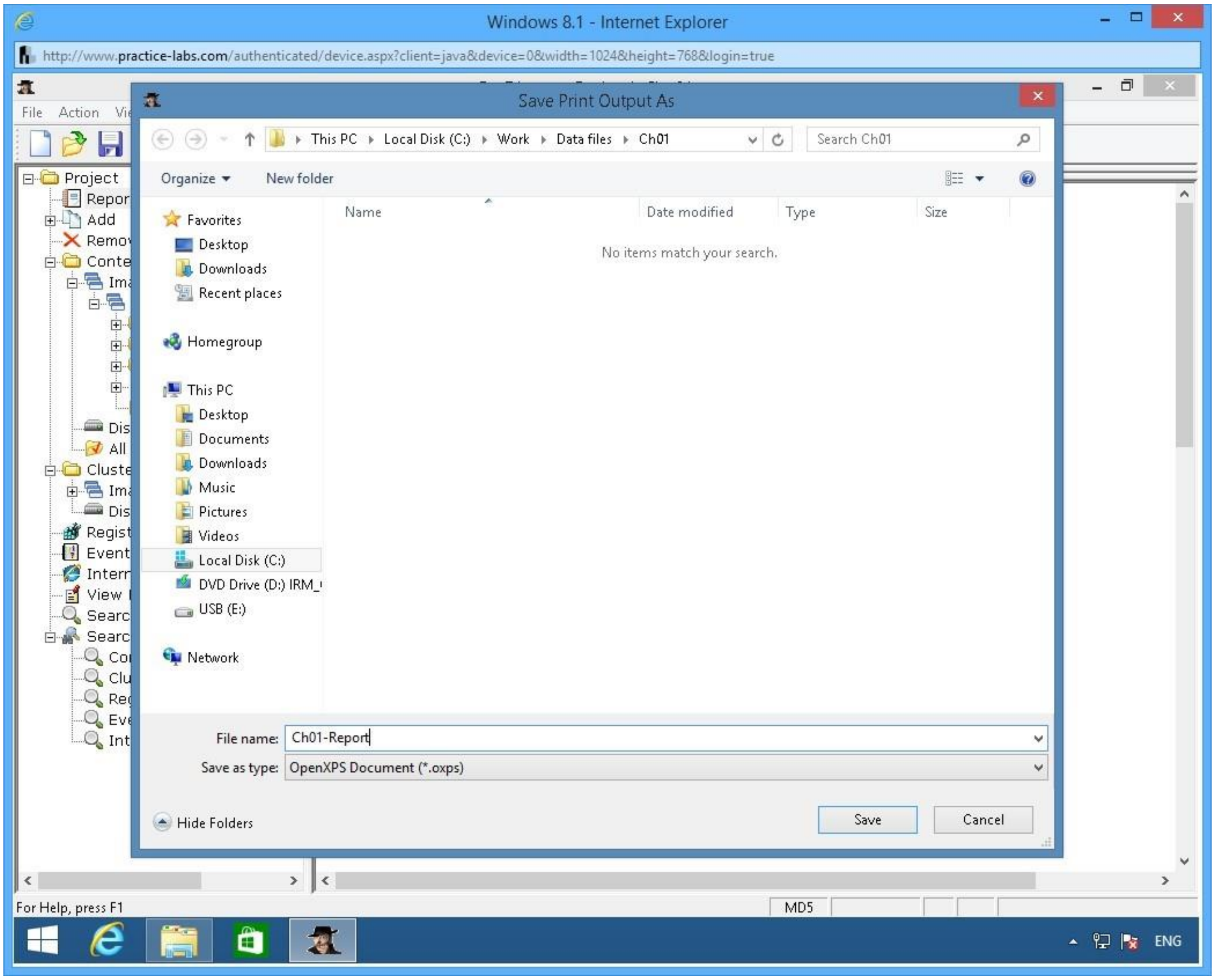


Bước 4

Trên hộp thoại **Lưu Dưới dạng Đầu ra In dưới dạng** , bấm vào hộp **Tên tệp** và nhập:

```
Ch01-Report
```

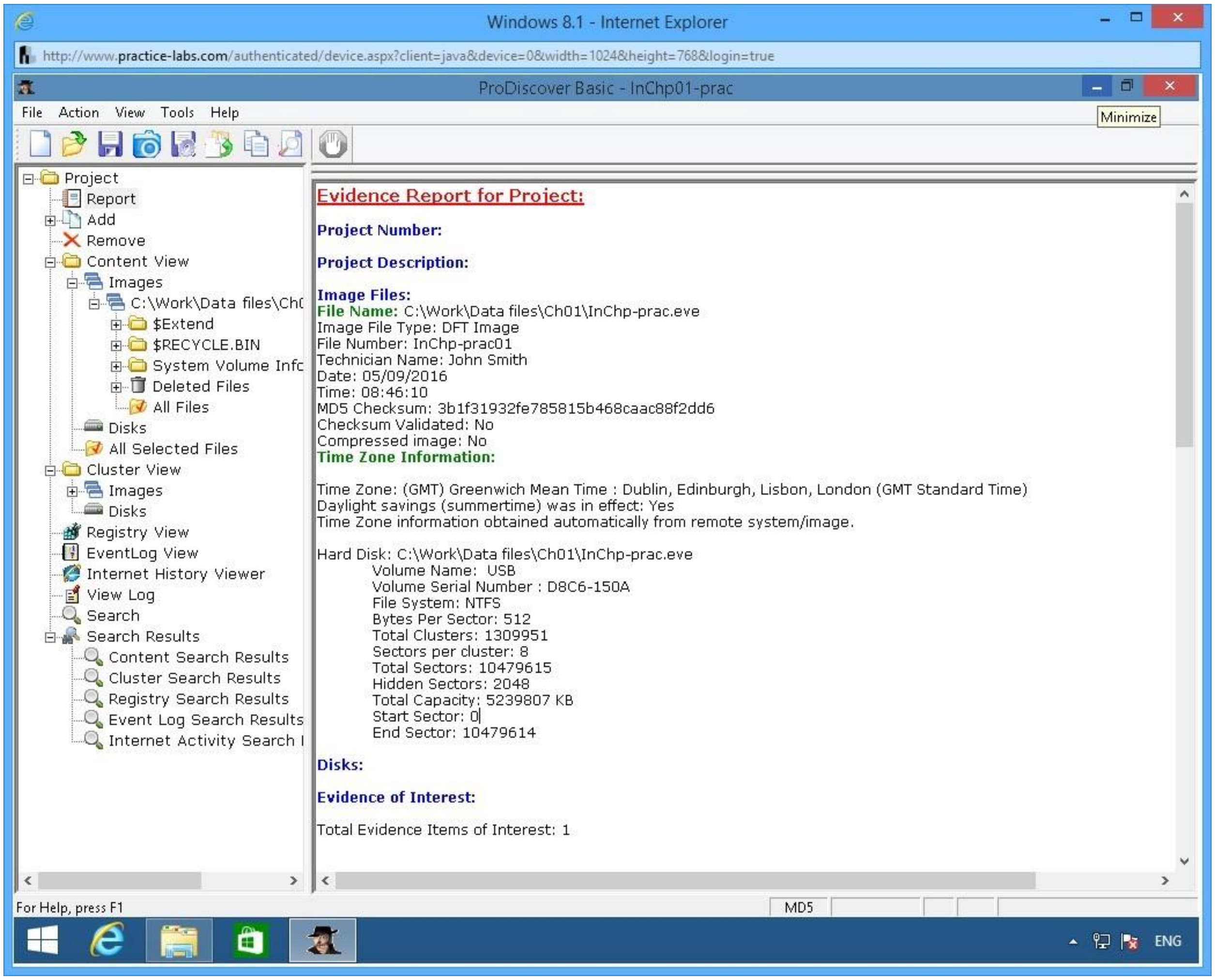
Nhấp vào **Lưu** .



Bước 5

Thu nhỏ Cửa sổ **ProDiscover Basic - InCh01-Practice** .

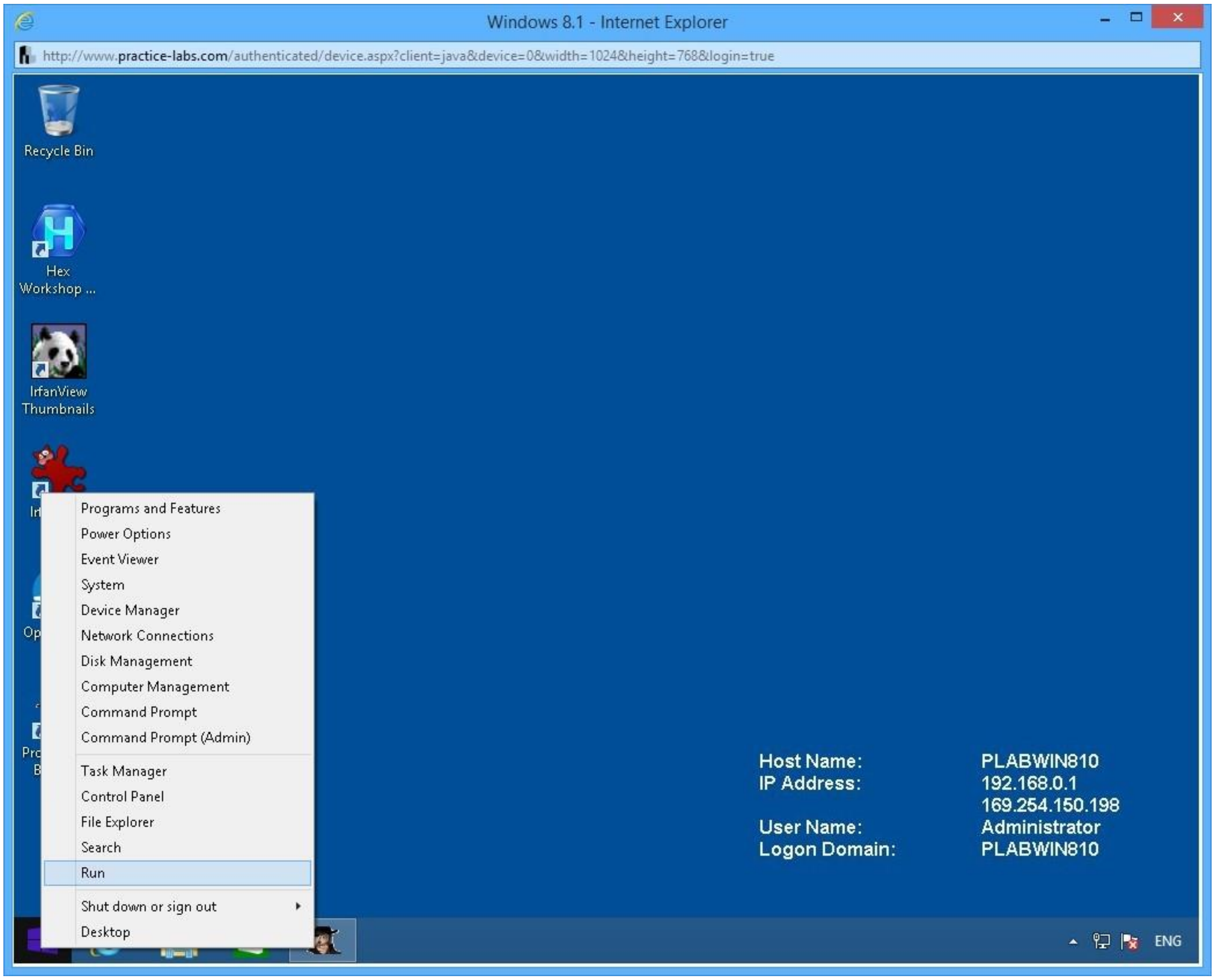
Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Bước 6

Bấm chuột phải vào **Bắt đầu** (Start) rồi trên menu lối tắt, bấm **Chạy** .

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



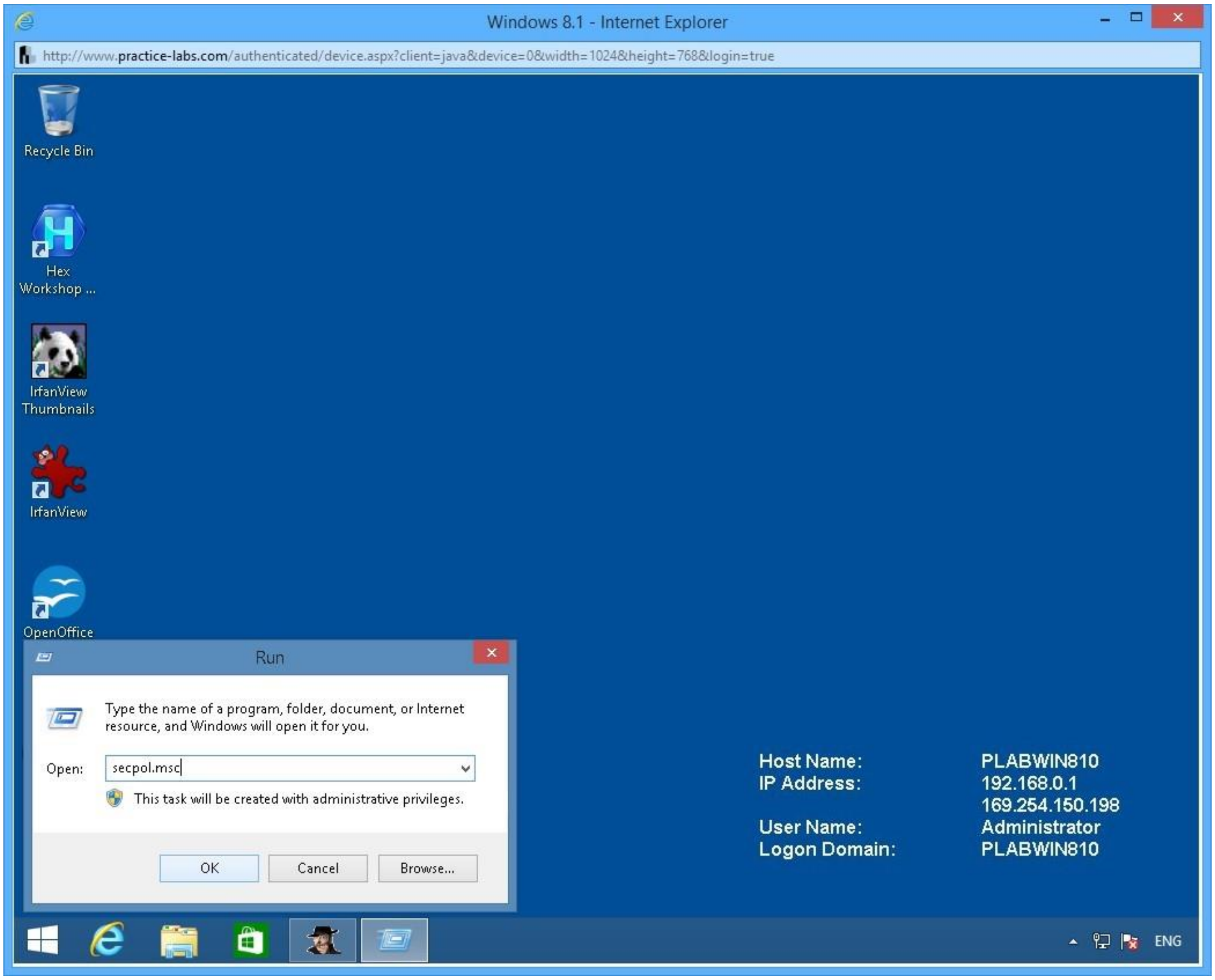
Bước 7

Bạn sẽ khởi chạy Chính sách bảo mật cục bộ và đặt chính sách cho phép Quản trị viên Open trình đọc XPS gốc trong Windows 8.1.

Trên hộp thoại **Chạy** , nhập:

```
secpol.msc
```

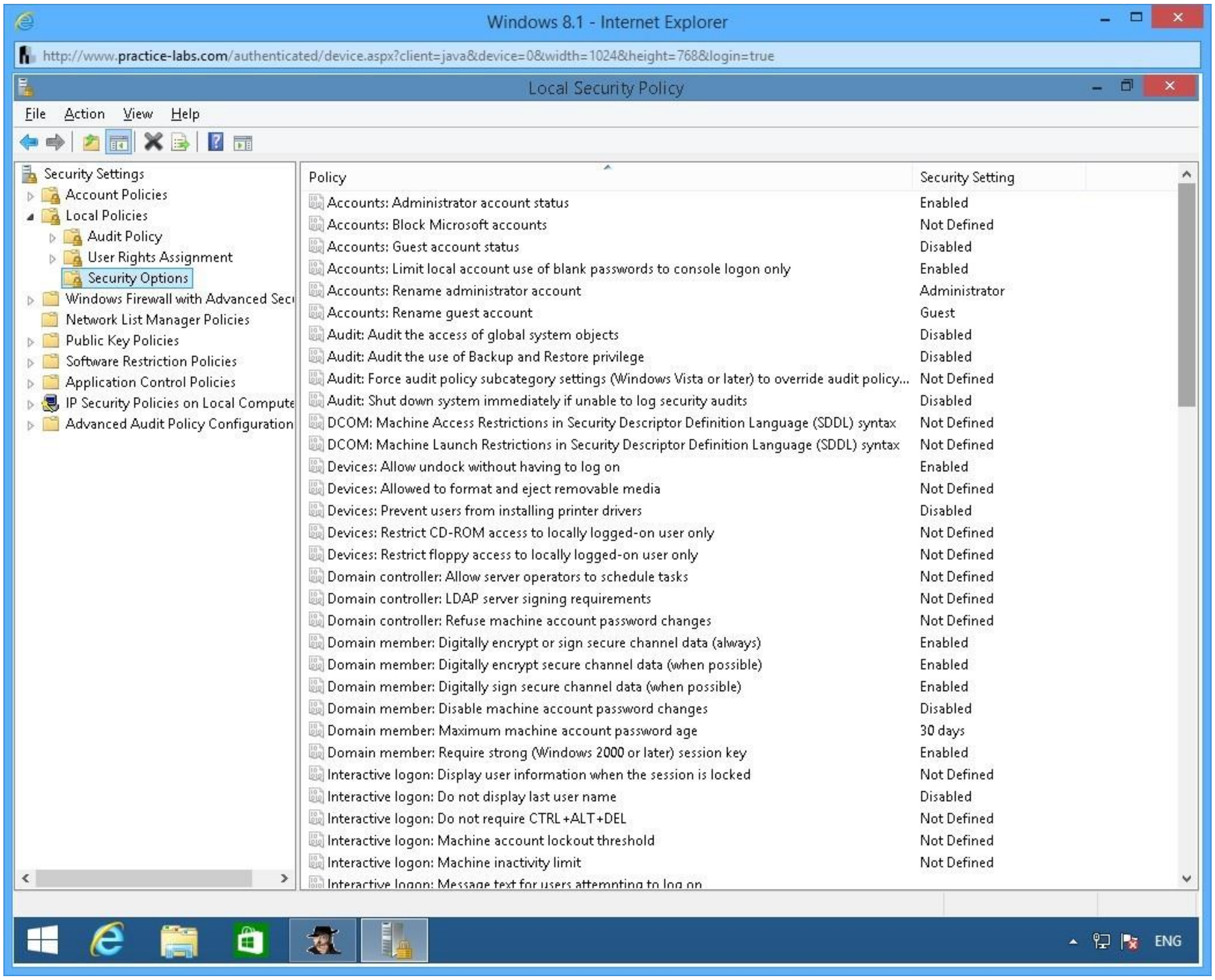
Nhấn **Enter** .



Bước 8

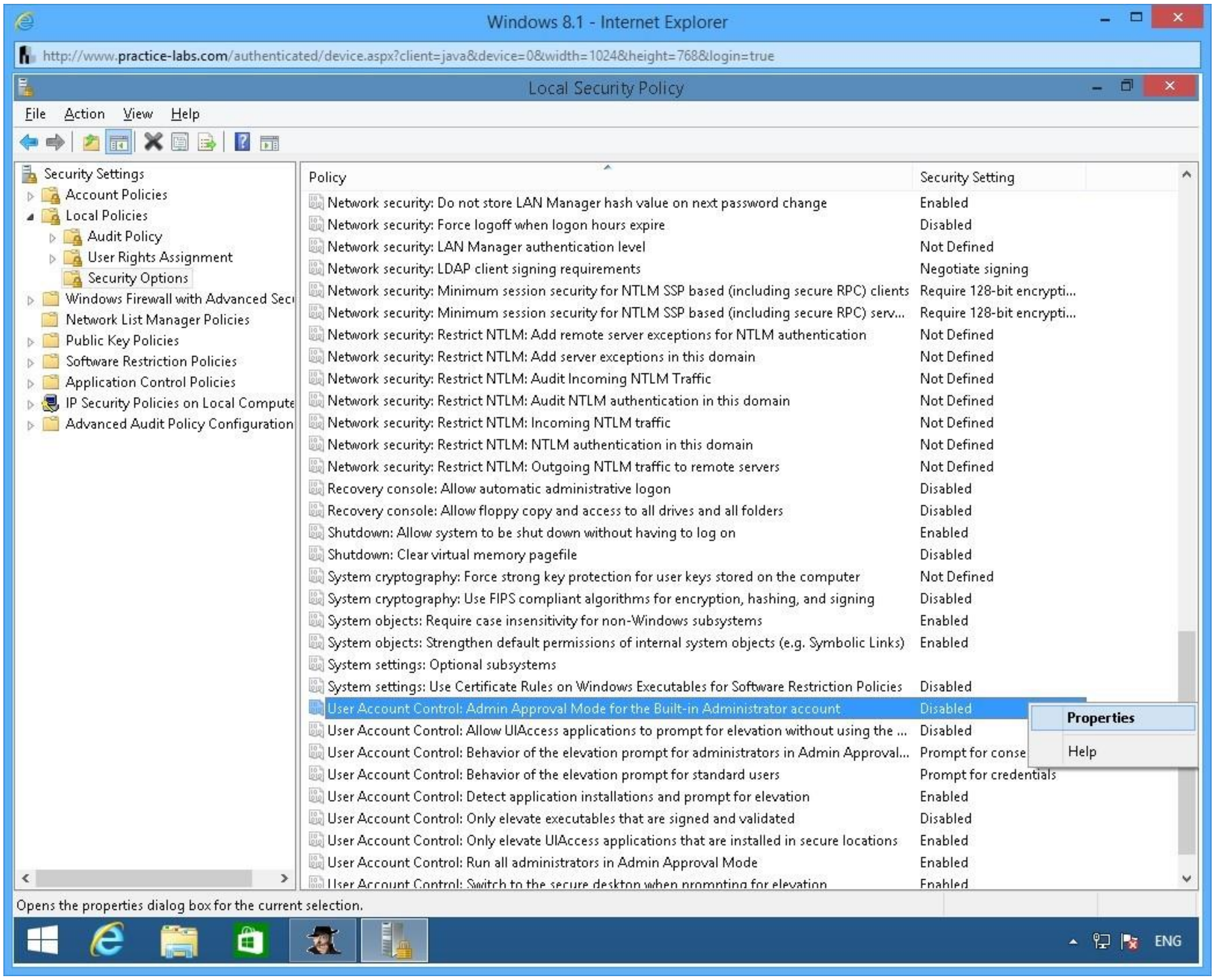
Trên cửa sổ **Chính sách bảo mật cục bộ** , Mở rộng **Chính sách cục bộ,** sau đó nhấp vào nút **Tùy chọn bảo mật** .

Trên ngăn chi tiết ở bên phải, cuộn xuống và tìm **Kiểm soát Tài khoản Người dùng: Chế độ Phê duyệt Quản trị viên cho tài khoản Quản trị viên Tích hợp** .



Bước 9

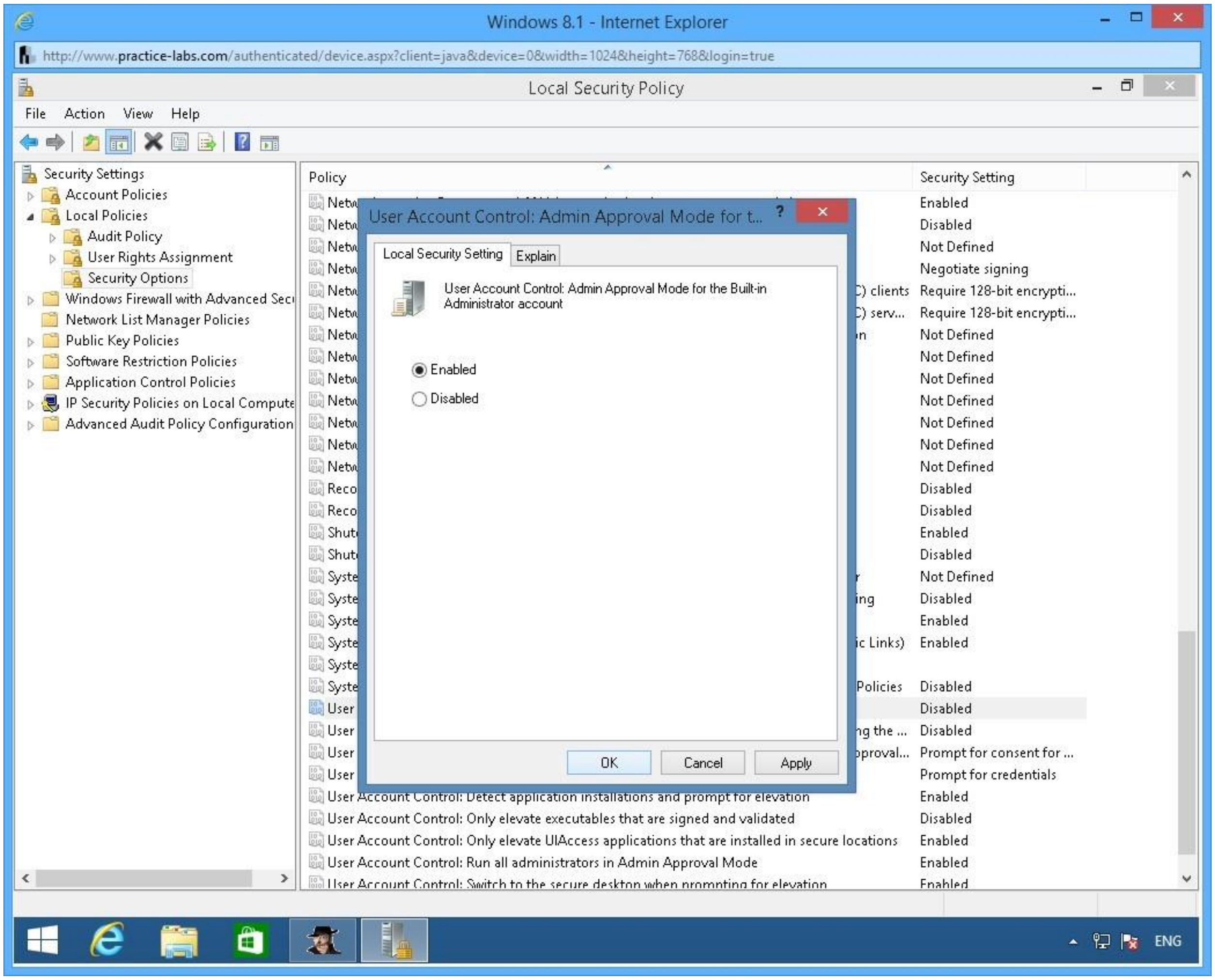
Nhấp chuột phải vào **Kiểm soát Tài khoản Người dùng: Chế độ Phê duyệt Quản trị viên cho** chính sách **tài khoản Quản trị viên Tích hợp** và chọn **Thuộc tính** .



Bước 10

Trên **Kiểm soát Tài khoản Người dùng: Chế độ Phê duyệt Quản trị viên cho** hộp thoại **Thuộc tính Tài khoản Quản trị viên Tích hợp** , chọn **Đã bật** (Enable).

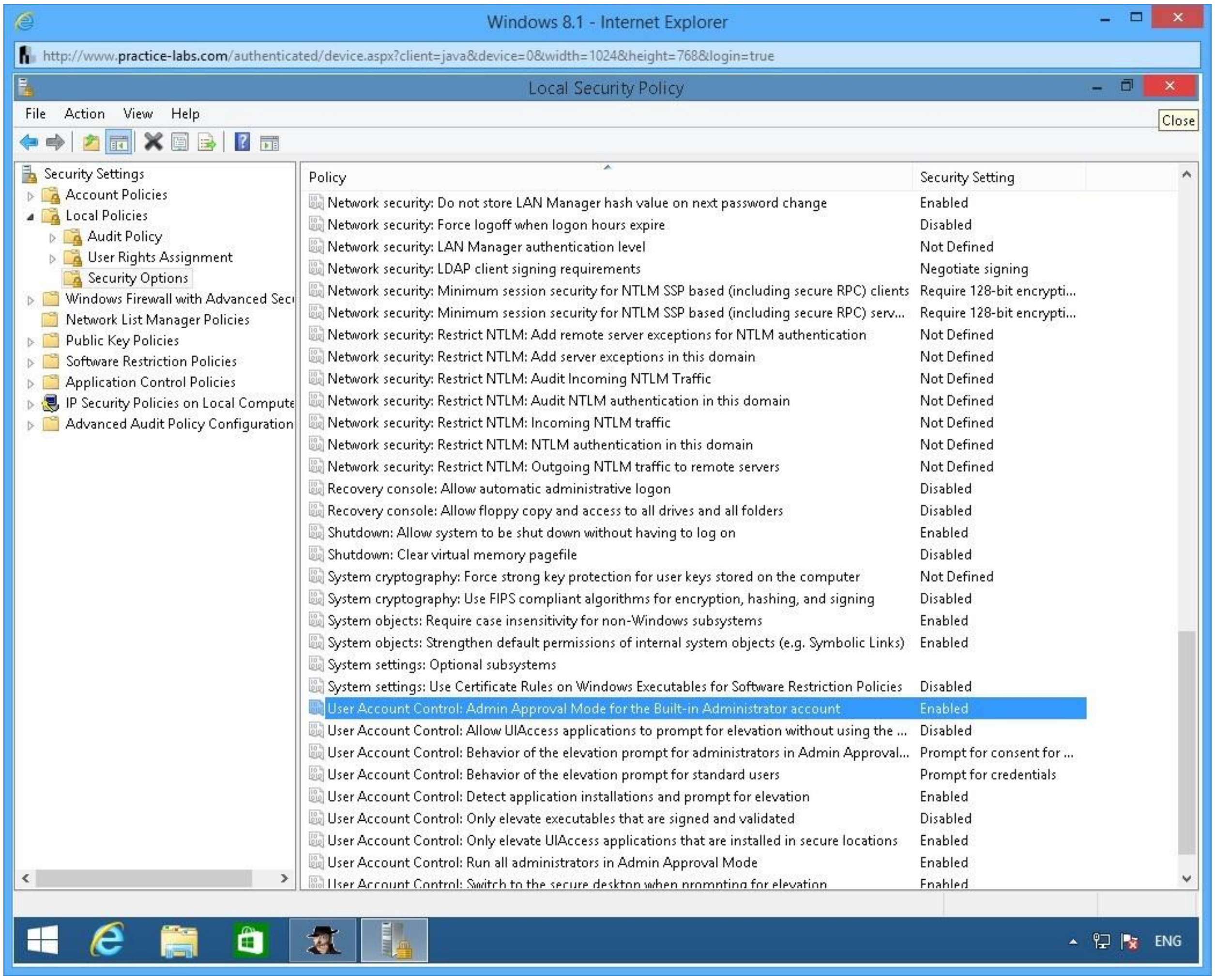
Bấm **OK** .



Bước 11

Đóng cửa sổ **Chính sách bảo mật cục bộ** (Local Security Policy).

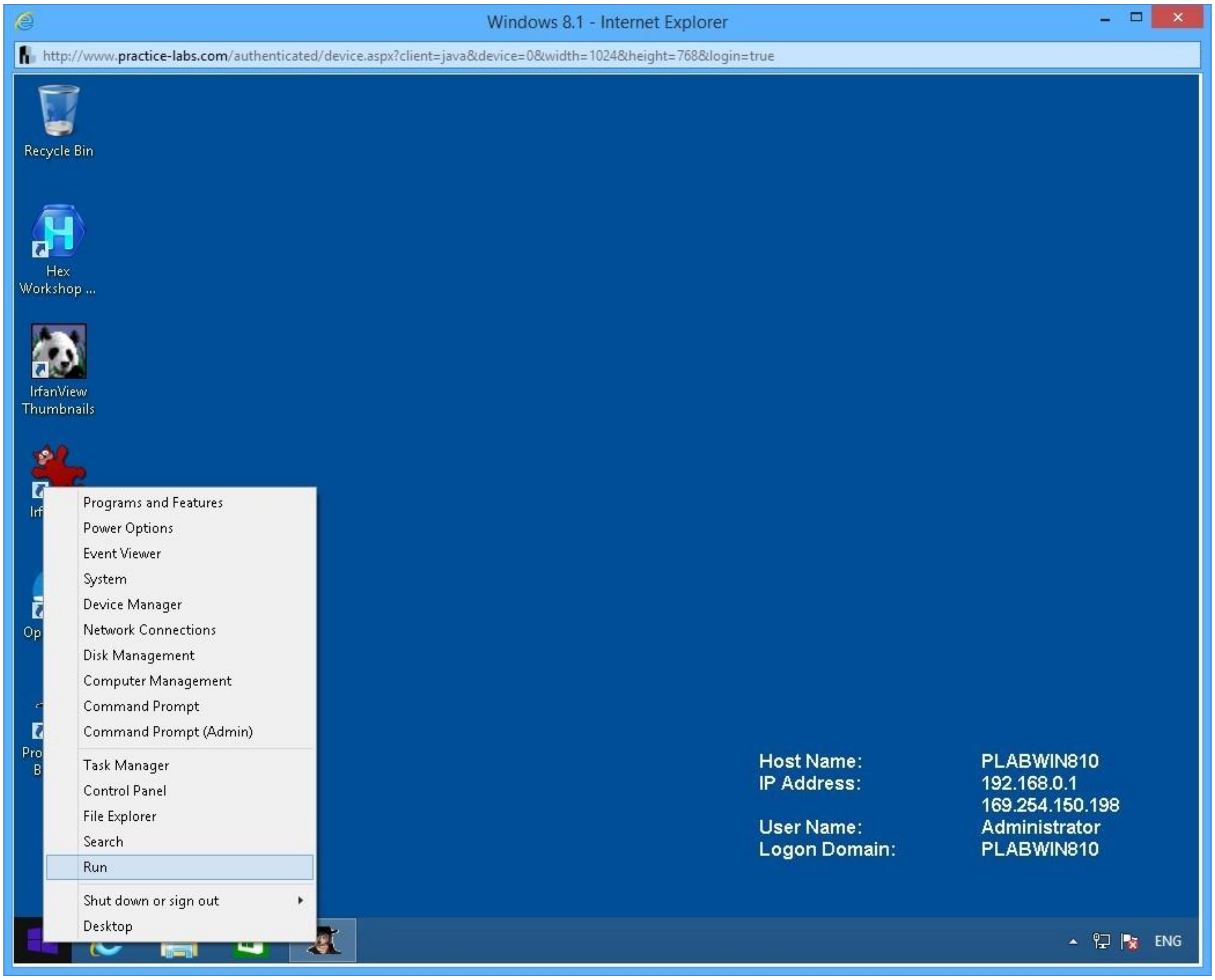
Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Bước 12

Nhấp chuột phải vào **Bắt đầu** và chọn **Chạy** .

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



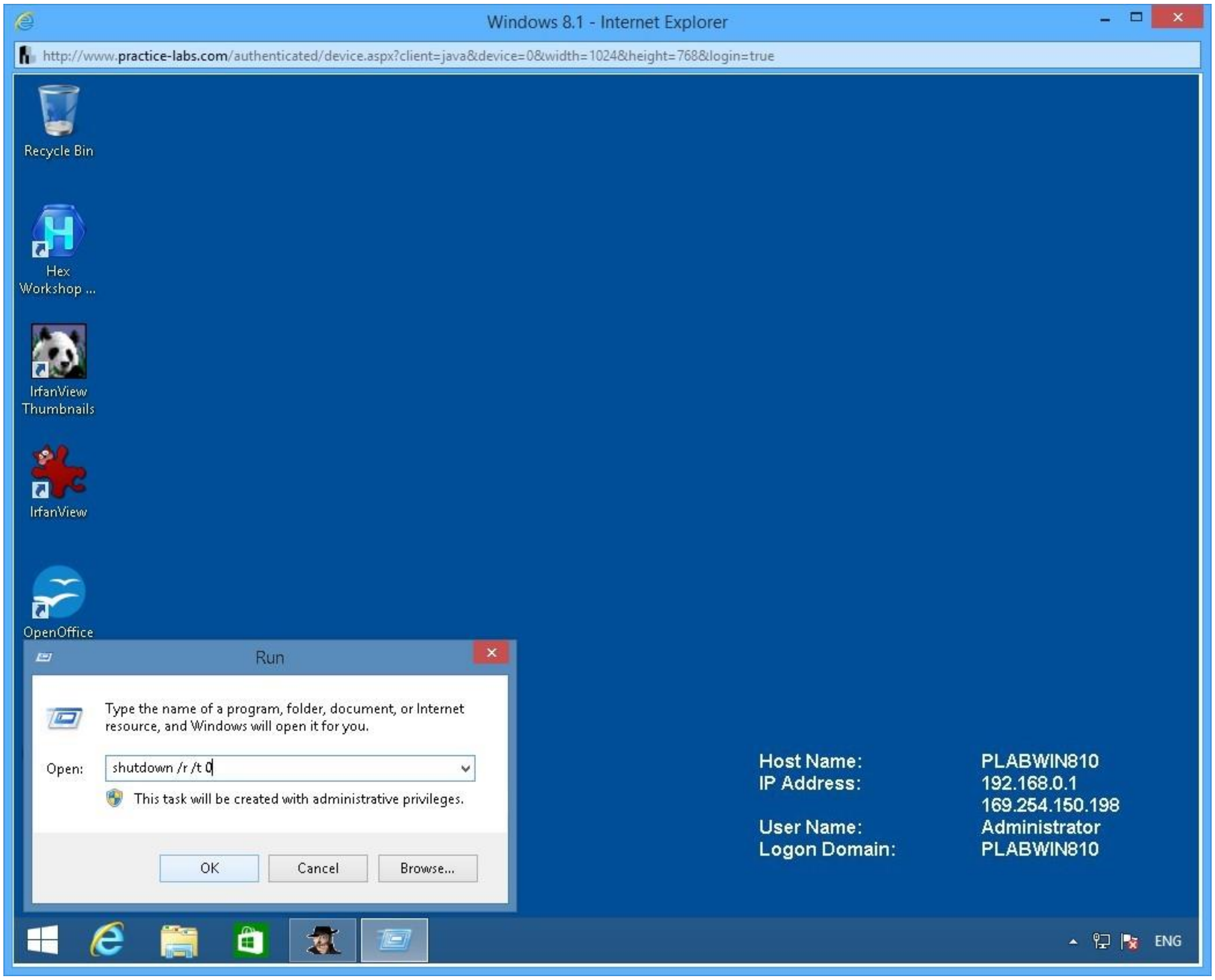
Bước 13

Trên hộp thoại **Chạy** , nhập:

```
shutdown /r /t 0
```

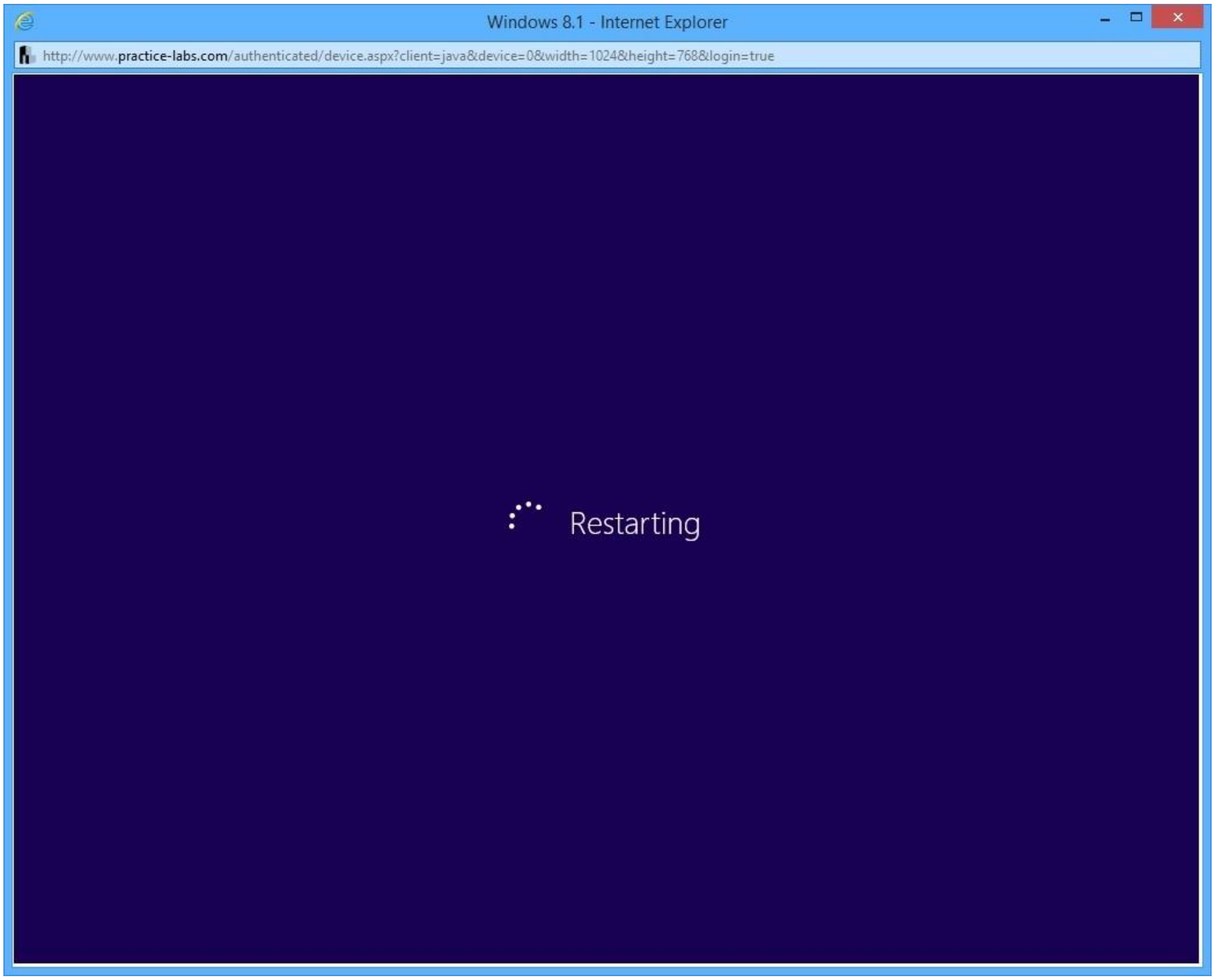
Nhấn **Enter** .

Bắt buộc phải khởi động lại máy tính để chính sách này áp dụng cho máy tính cục bộ.



Bước 14

Vui lòng đợi trong khi **PLABWIN810** được khởi động lại.



Giữ cho thiết bị được bật nguồn ở trạng thái hiện tại và tiến hành tác vụ tiếp theo.

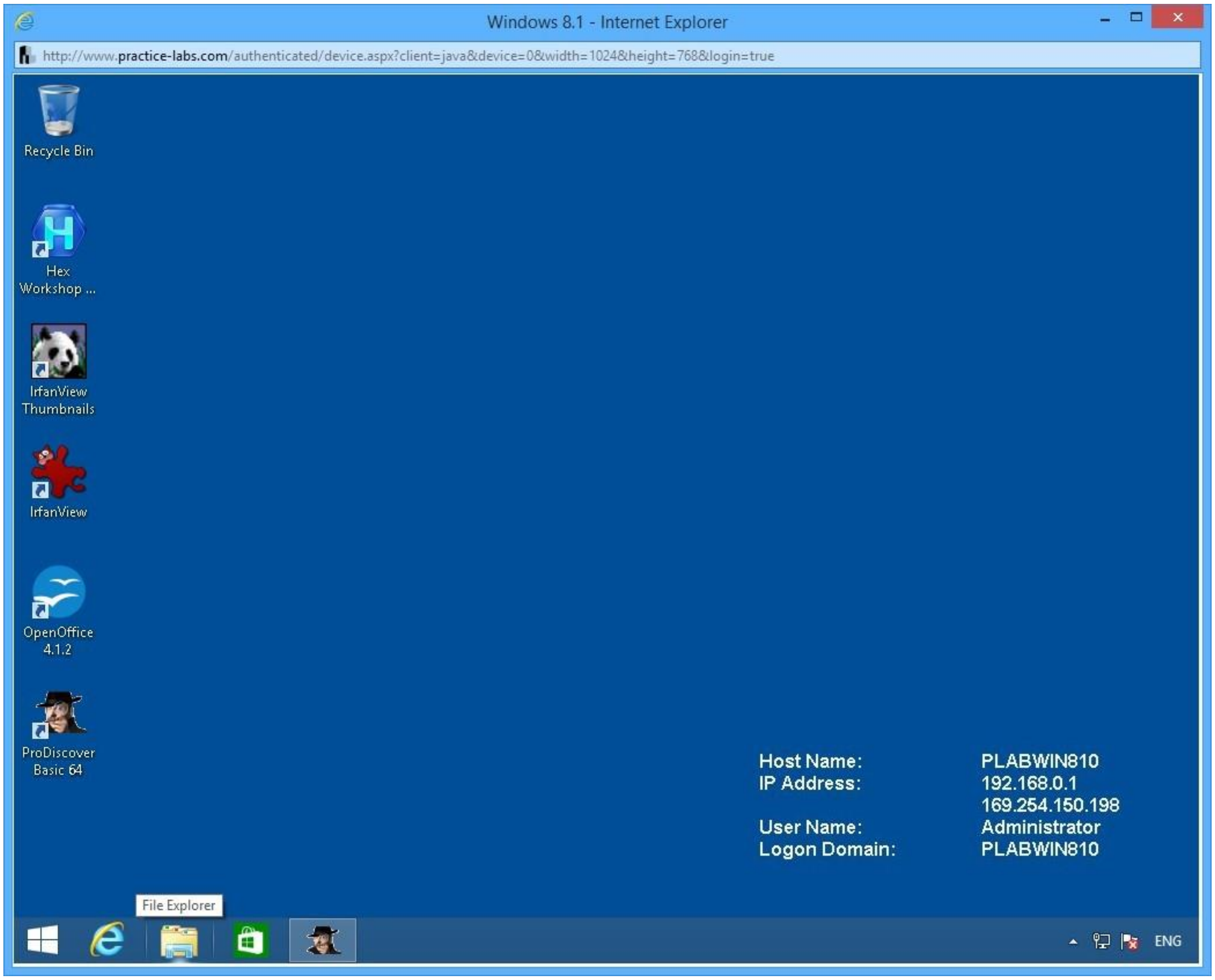
Nhiệm vụ 4 - Xem Report

Để đọc Report được tạo từ ProDiscover Basic, hãy làm theo các bước sau:

Bước 1

Kết nối lại với thiết bị **PLABWIN810** sau khi khởi động lại.

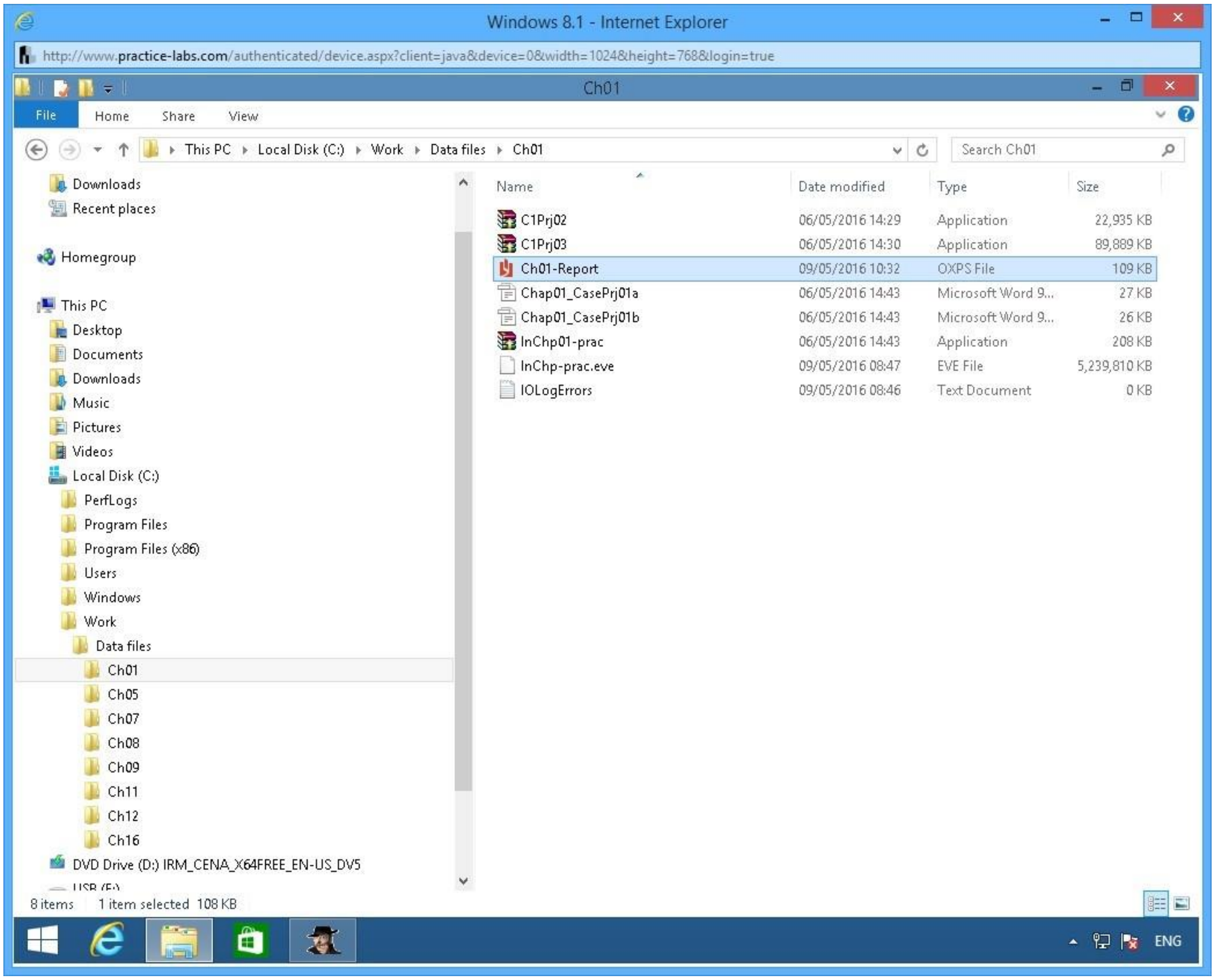
Khi đã đăng nhập, hãy nhấp vào biểu tượng **File Explorer** trên thanh tác vụ.



Bước 2

Trên cửa sổ **File Explorer** , Mở rộng **Local Disk C> Work> Data files,** sau đó nhấp vào thư mục **Ch01** .

Trên ngăn chi tiết ở bên phải, bấm đúp vào **Ch01-Report** .

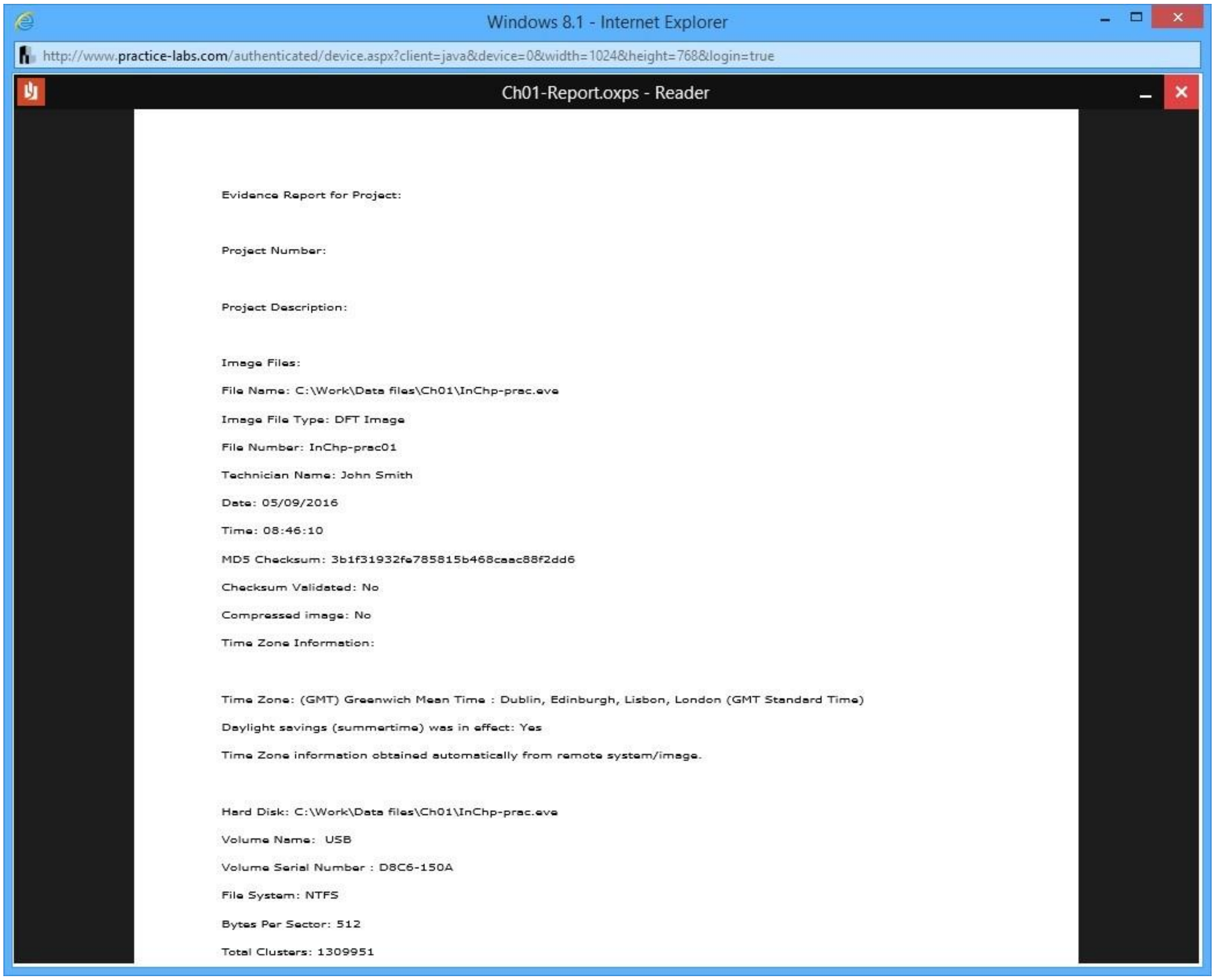


Bước 3

Trình đọc XPS gốc của Windows 8.1 sẽ Open Report.

Di chuột trên đầu màn hình cho đến khi bạn nhìn thấy thanh tiêu đề.

Nhấp vào nút **[X]** để thoát khỏi ứng dụng khi xem xong nội dung của Report.



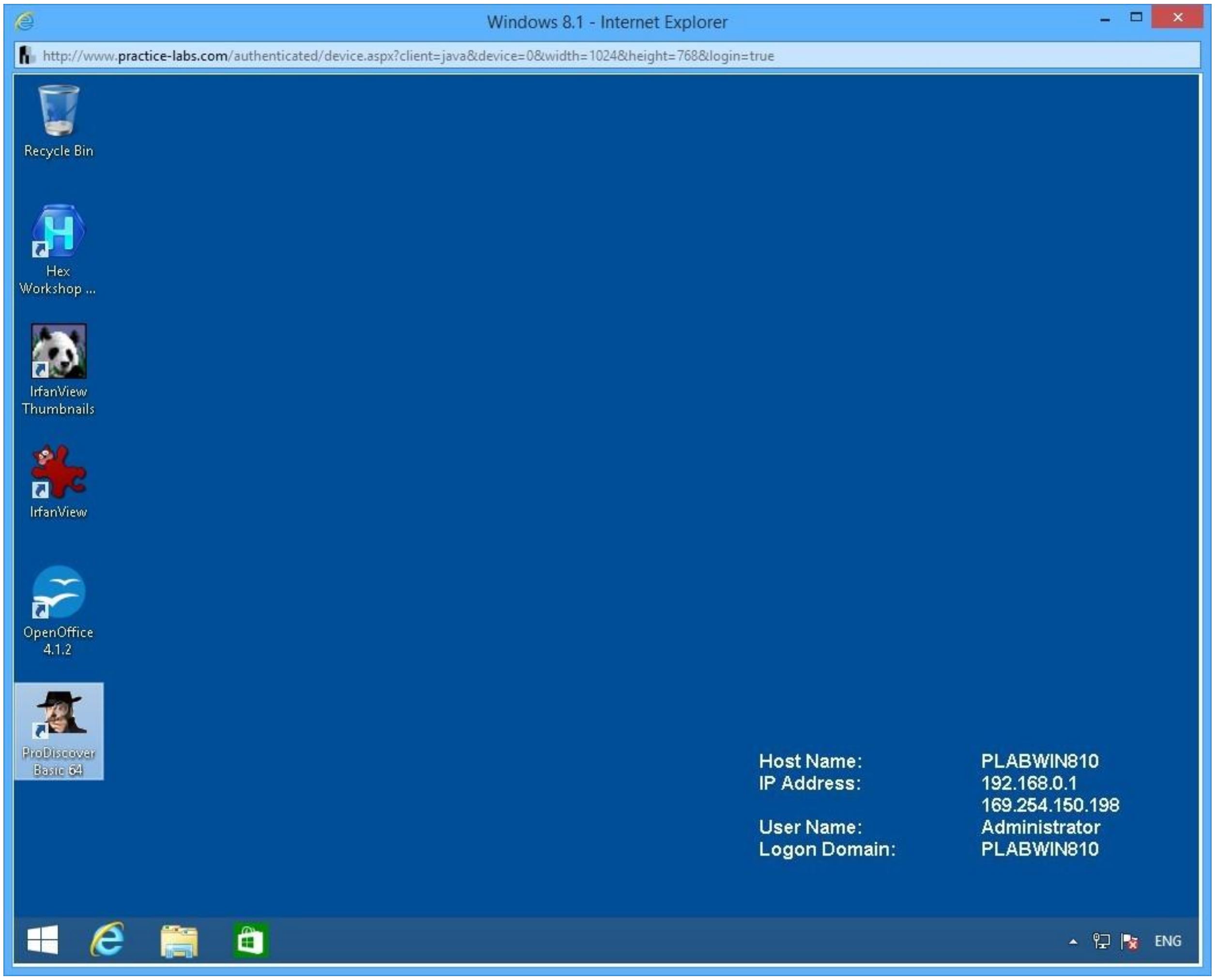
Giữ cho thiết bị được bật nguồn ở trạng thái hiện tại và tiến hành tác vụ tiếp theo.

Nhiệm vụ 5 - Xuất Report

Nếu Report cần được lưu vào tệp, bạn sử dụng tính năng Xuất của ProDiscover Basic và chọn RTF hoặc plaintext cho định dạng tệp. Để xuất Report thành tệp, hãy làm như sau:

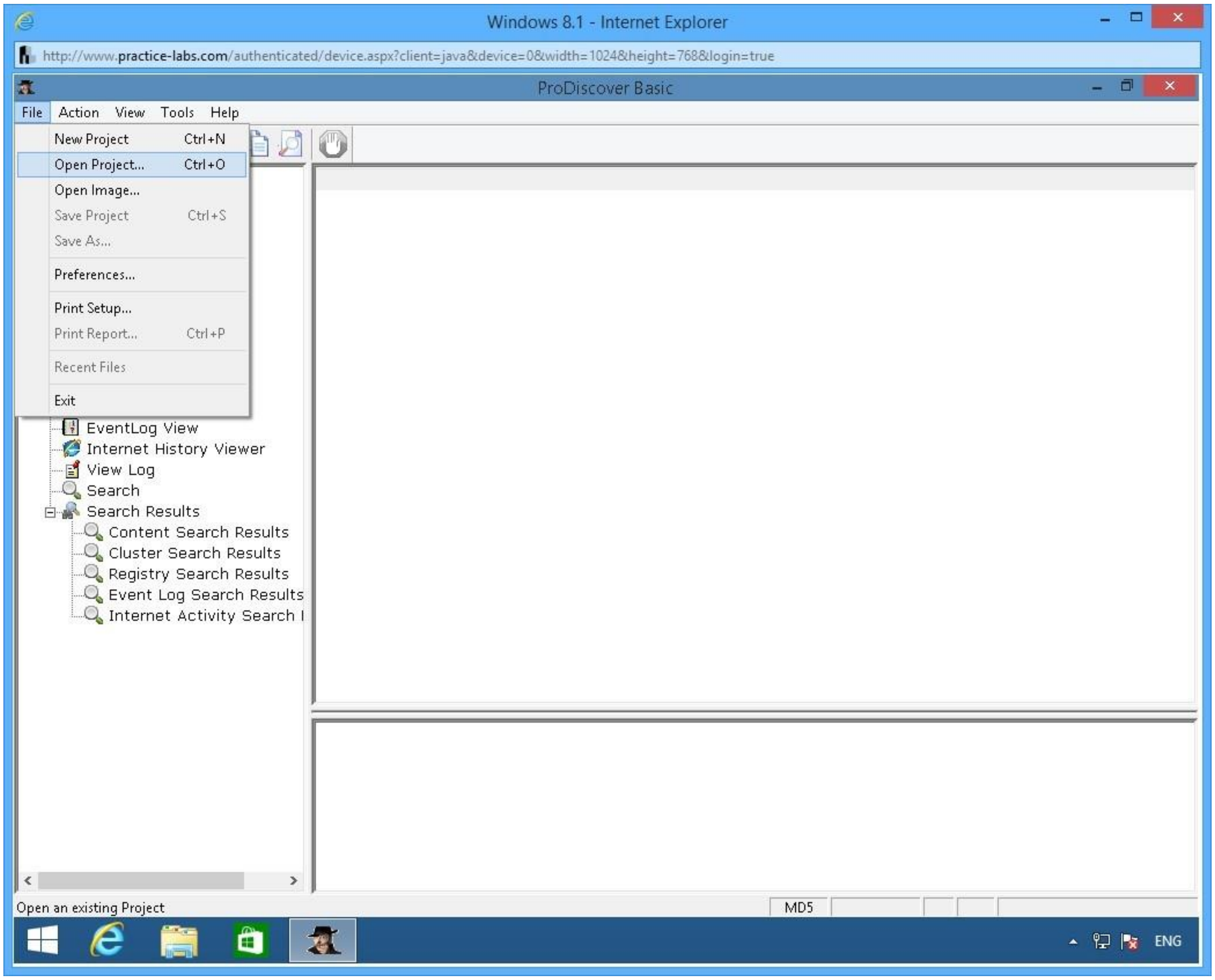
Bước 1

Trên thiết bị **PLABWIN810** , khởi chạy ứng dụng **ProDiscover Basic 64** từ máy tính để bàn.



Bước 2

Nhấp vào **Tệp** (File) và chọn **Open Dự án** (Open Project).

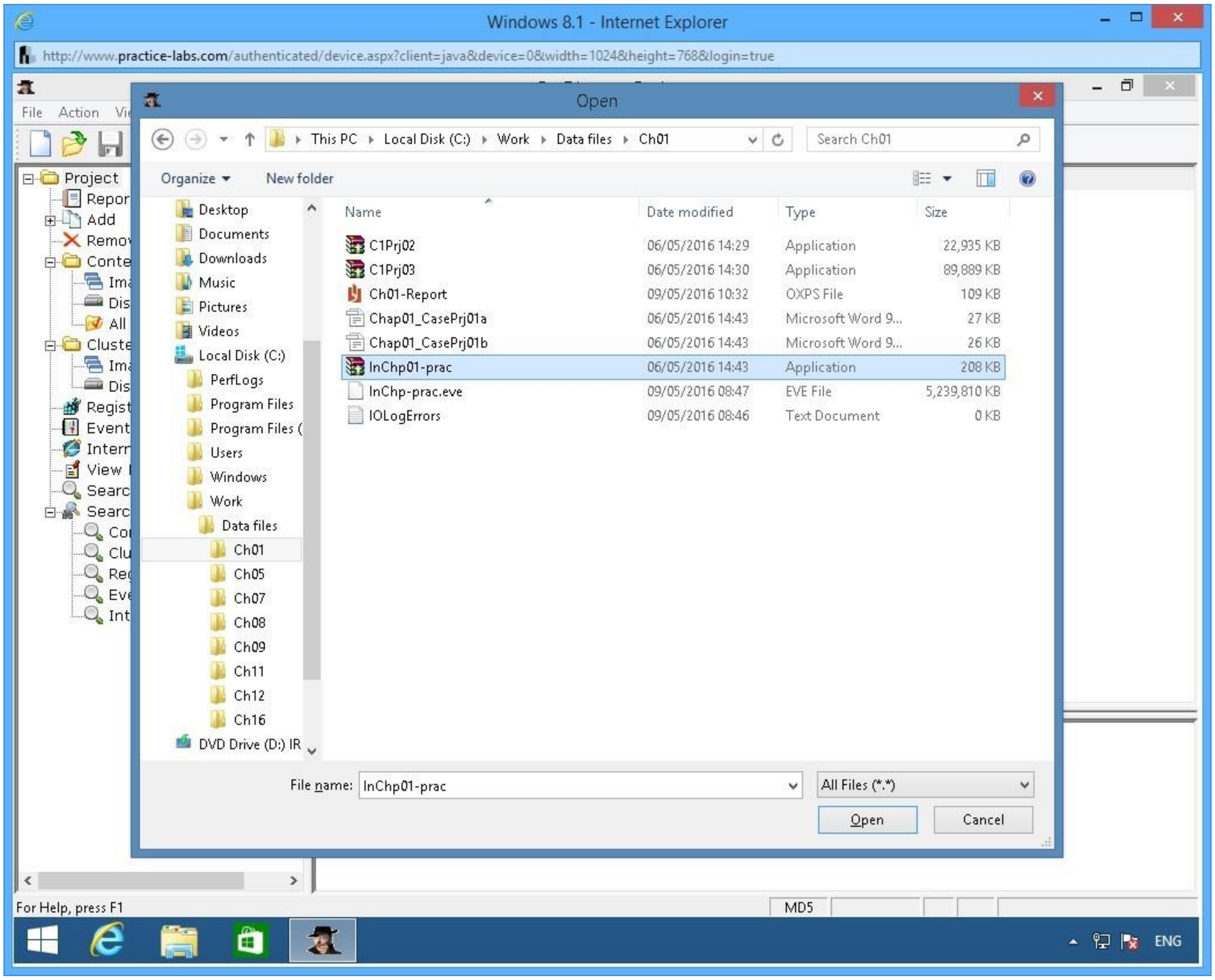


Bước 3

Trên hộp thoại Open , Mở rộng **Local Disk C> Work> Data files** rồi nhấp vào thư mục **Ch01** .

Ở phần dưới bên phải, tìm danh sách thả xuống và chọn **Tất cả tệp** (*. *).

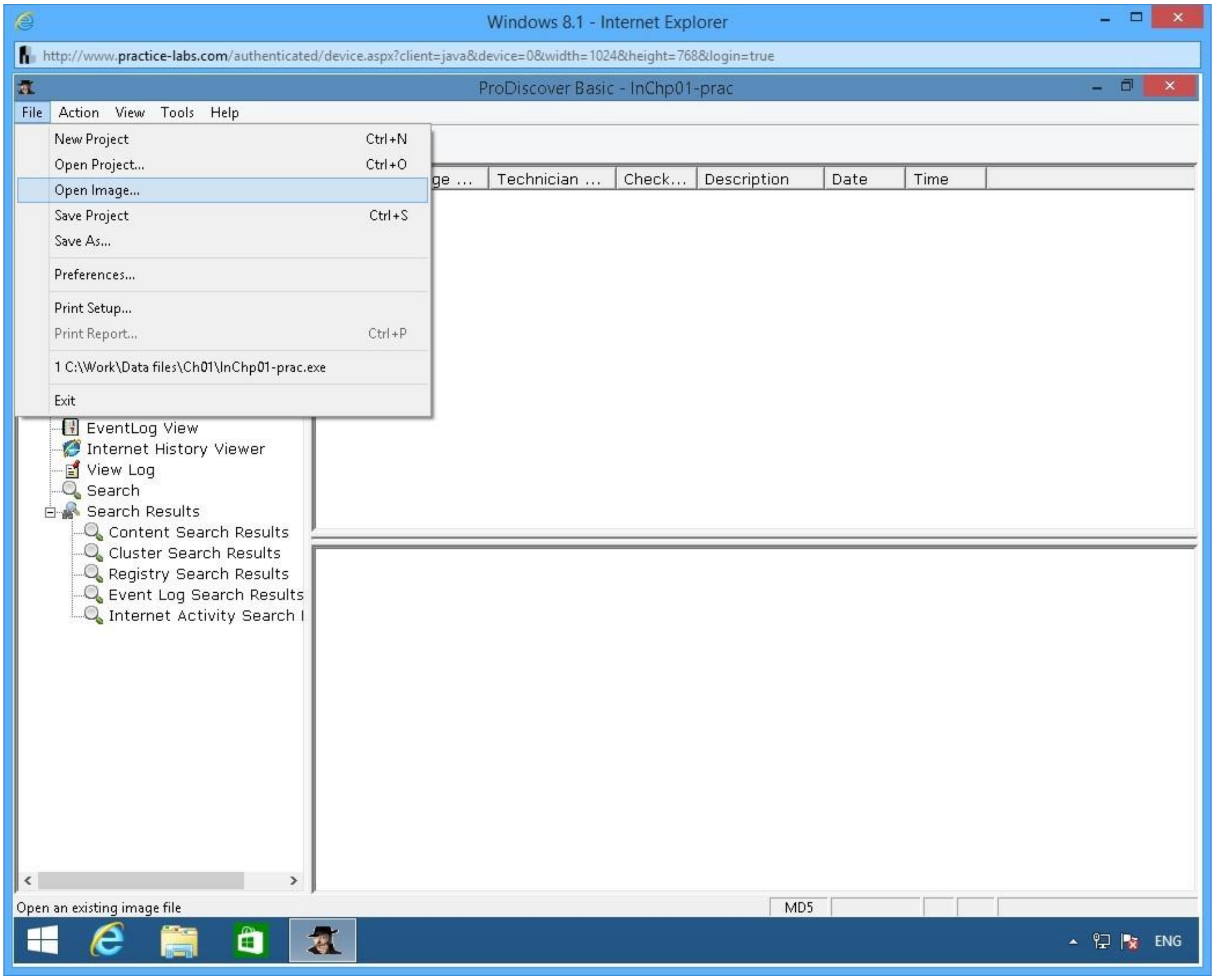
Từ danh sách các tệp, chọn **tệp InChp01-Practice** và nhấp vào **Open** (Open).



Bước 4

Khi dự án đang Open, bạn cần thêm các hình ảnh một lần nữa.

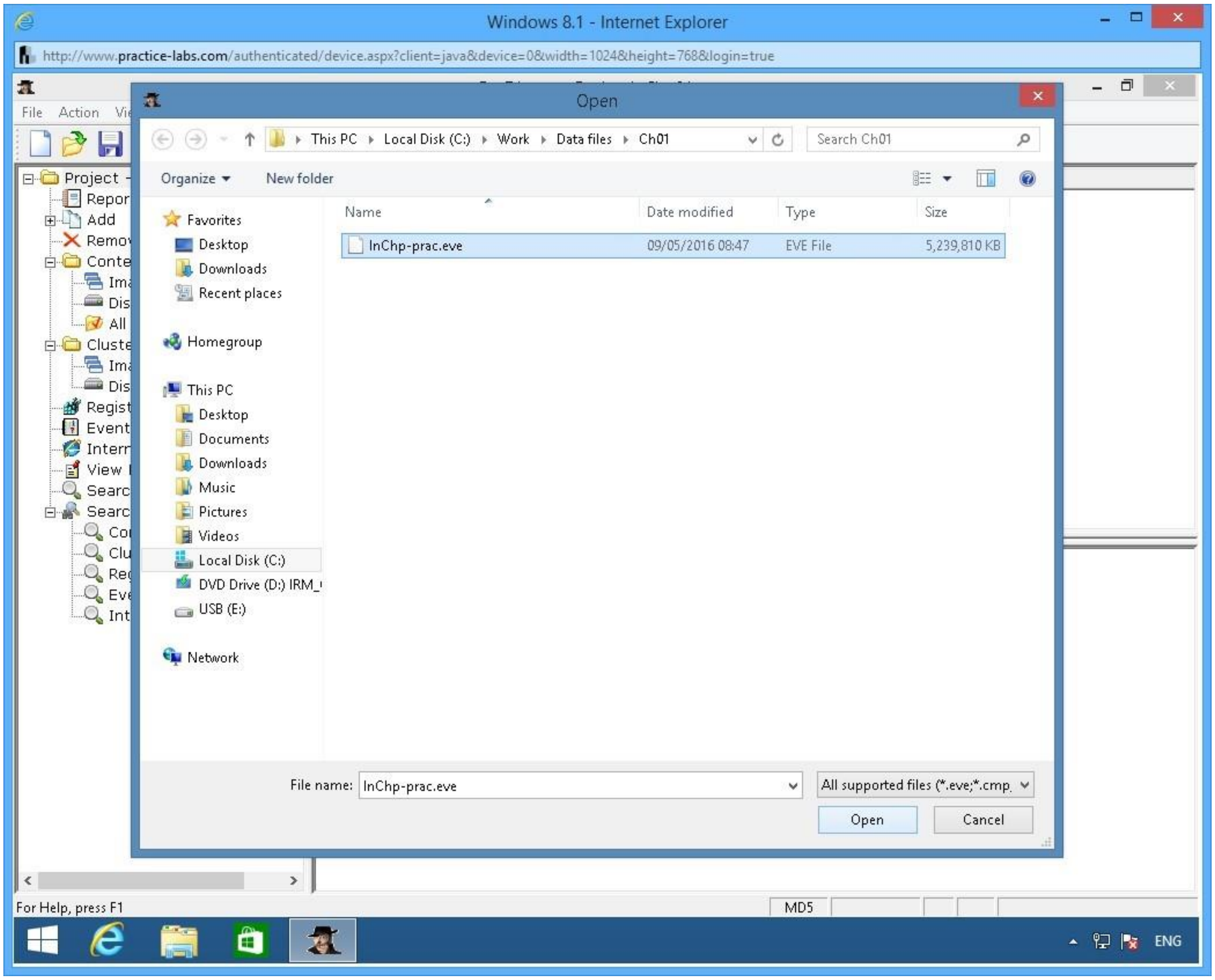
Nhấp vào **Tệp** và chọn **Open Hình ảnh** .



Bước 5

Trên hộp thoại Open , xác minh rằng bạn đang ở trong đường dẫn thư mục này: **Local Disk C> Work> Data files> Ch01** .

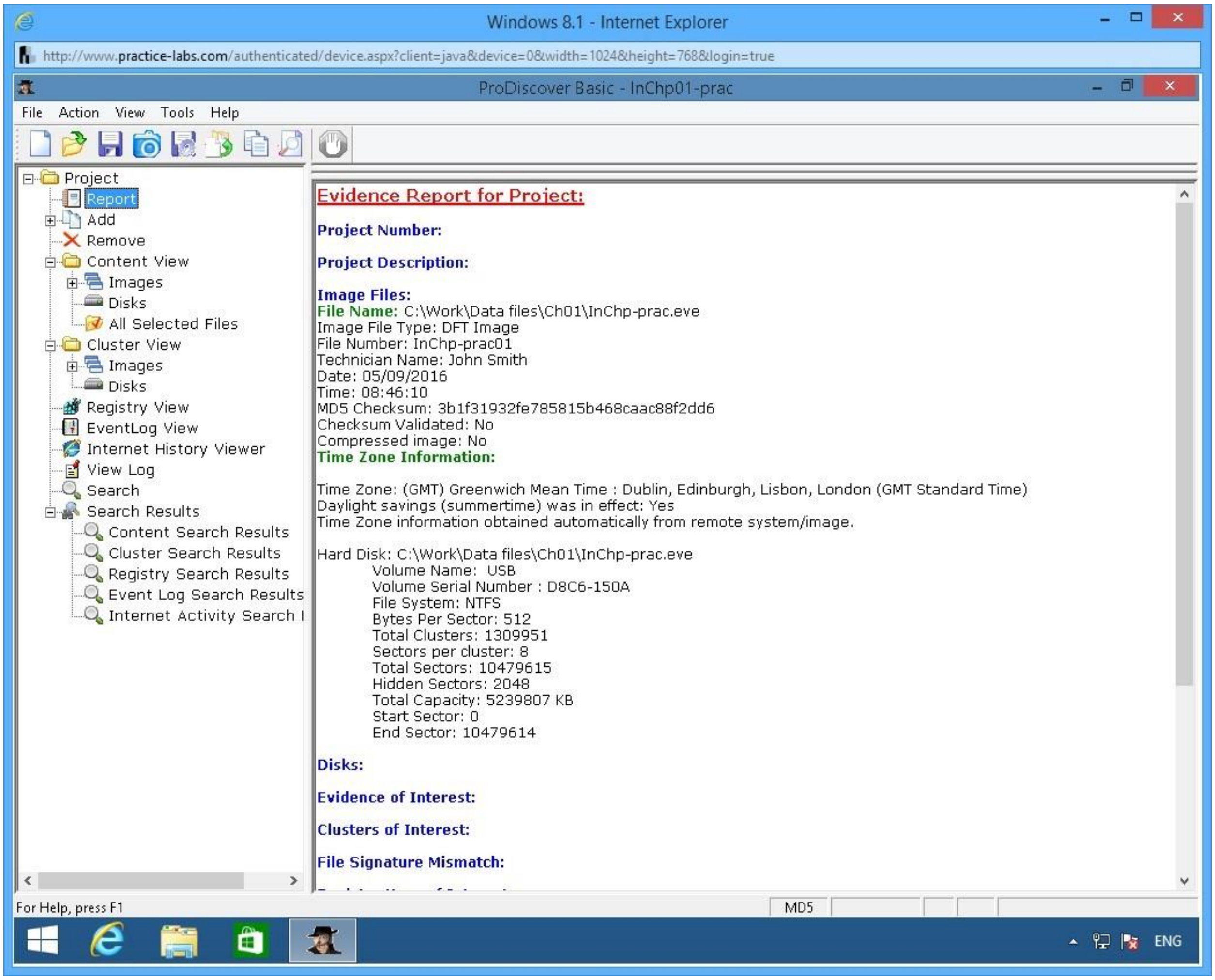
Chọn **InChp-Practice.eve** và nhấp vào **Open** .



Bước 6

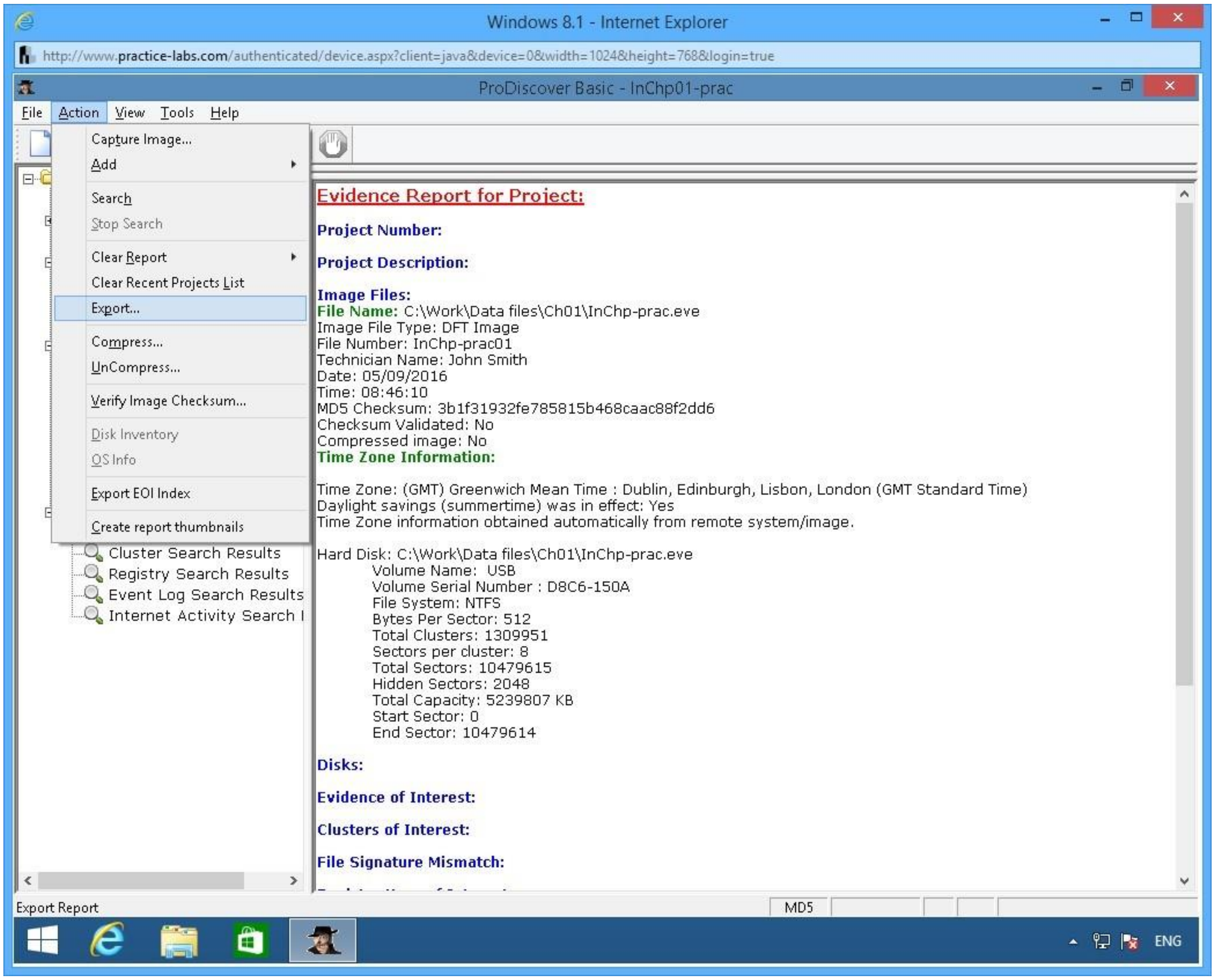
Sau khi Open hình ảnh, trong chế độ xem dạng cây, hãy nhấp vào **Report** .

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Bước 7

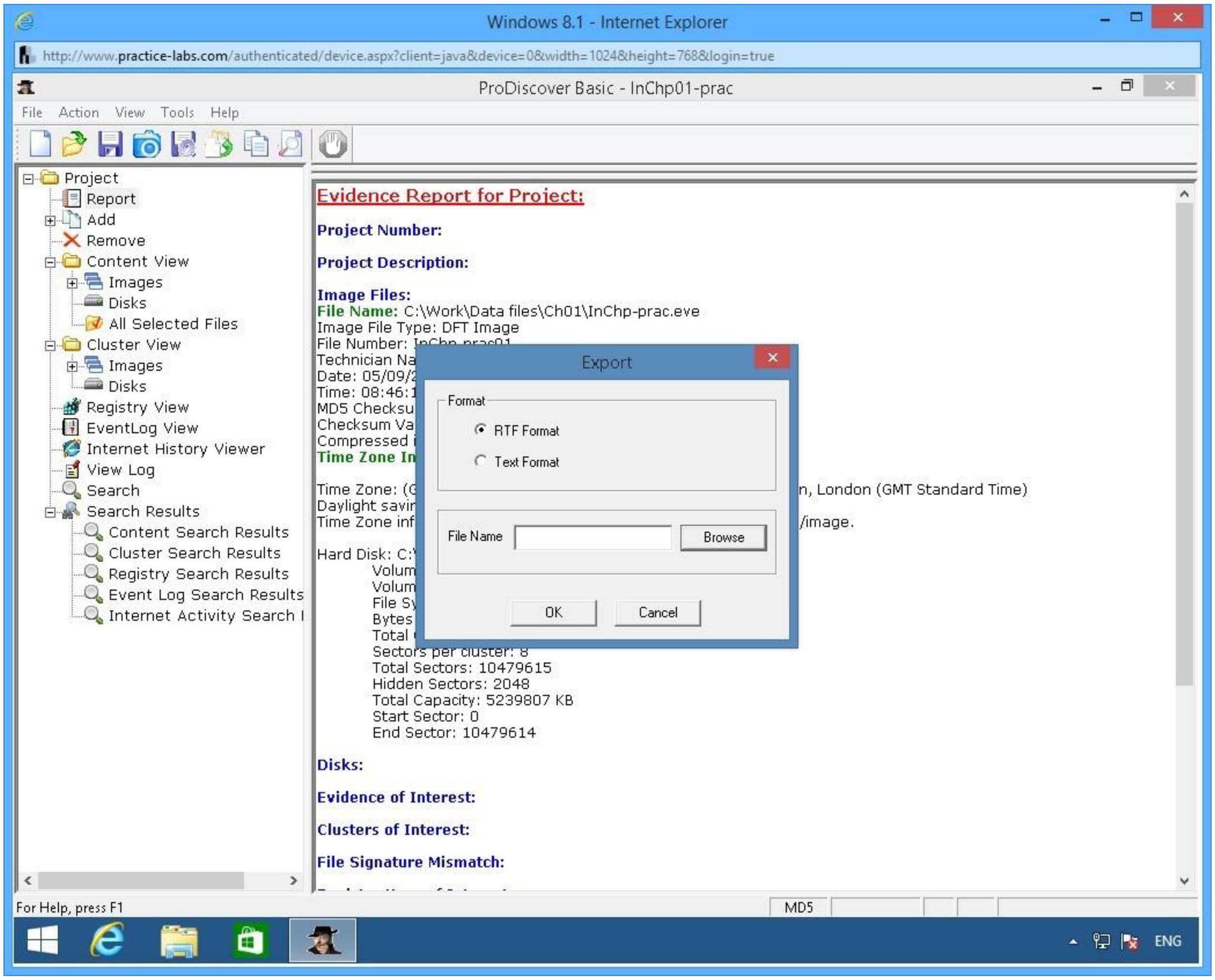
Nhấp vào **Action** , **Export** từ menu.



Bước 8

Trong hộp thoại **Export** , bấm vào nút tùy chọn **Định dạng RTF** , sau đó bấm **Duyệt** .

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



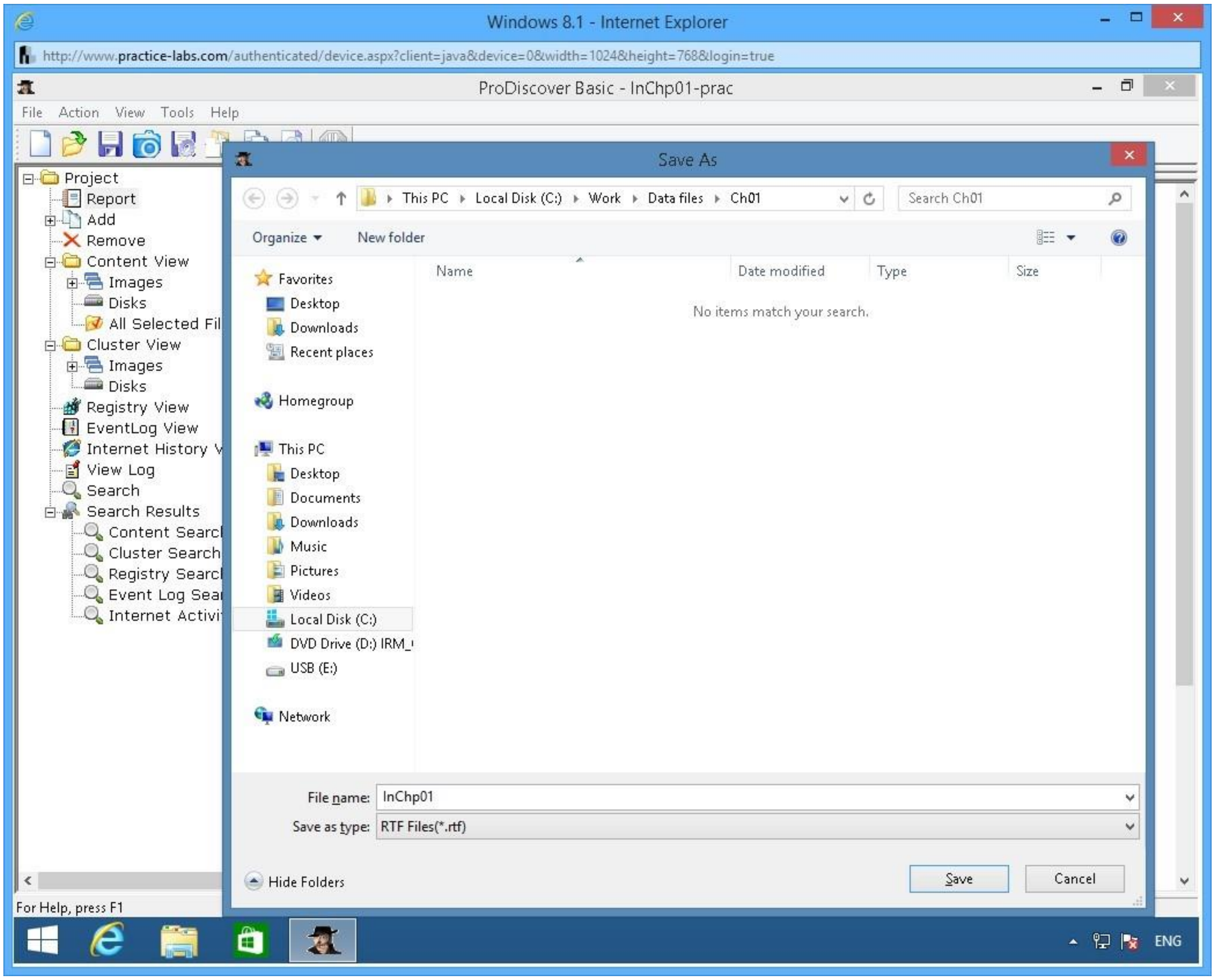
Bước 9

Trên hộp thoại **Lưu dưới dạng** , trong hộp văn bản **Tên tệp,** nhập vào :

```
InChp01
```

Nhấp vào **Lưu** .

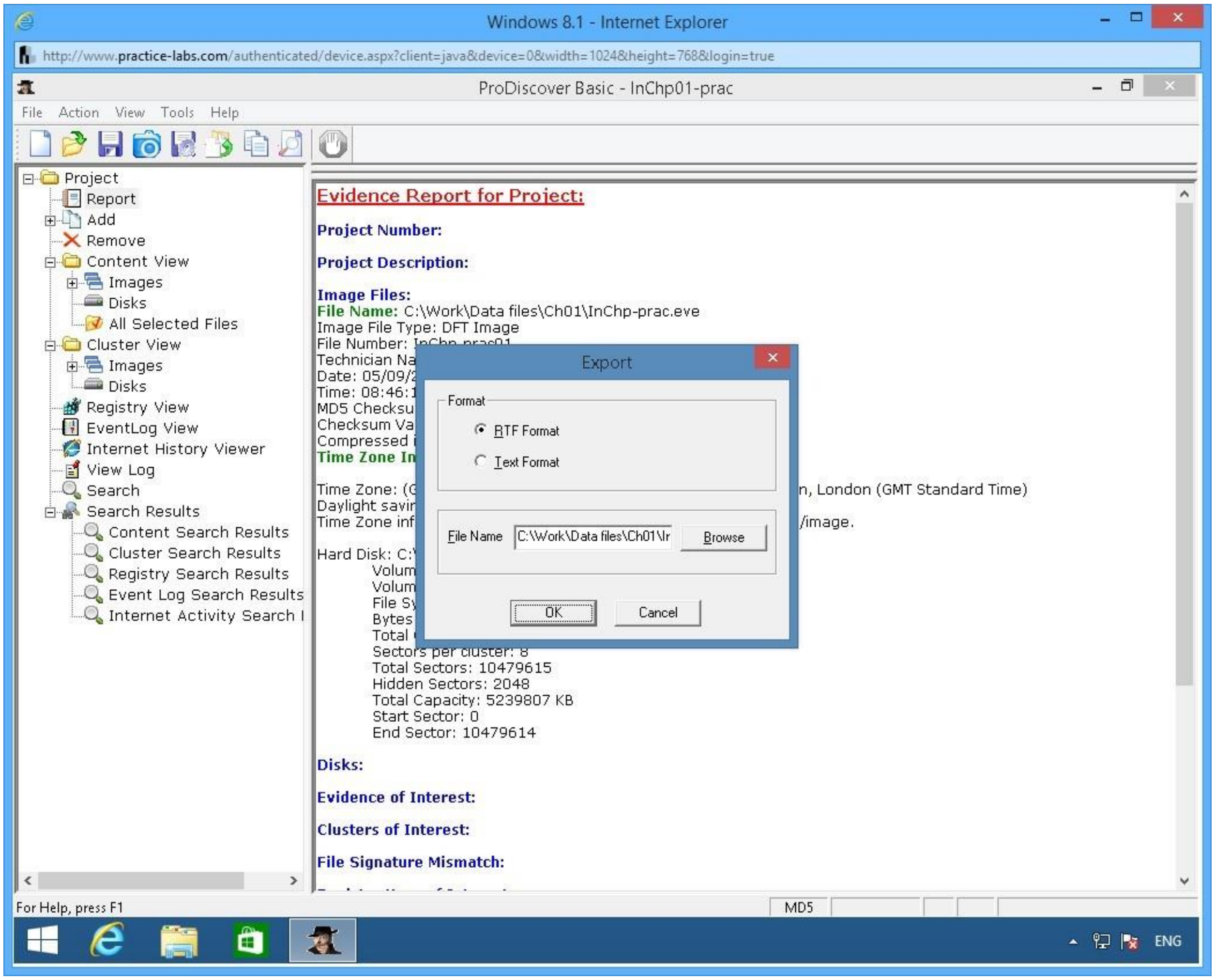
Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Bước 10

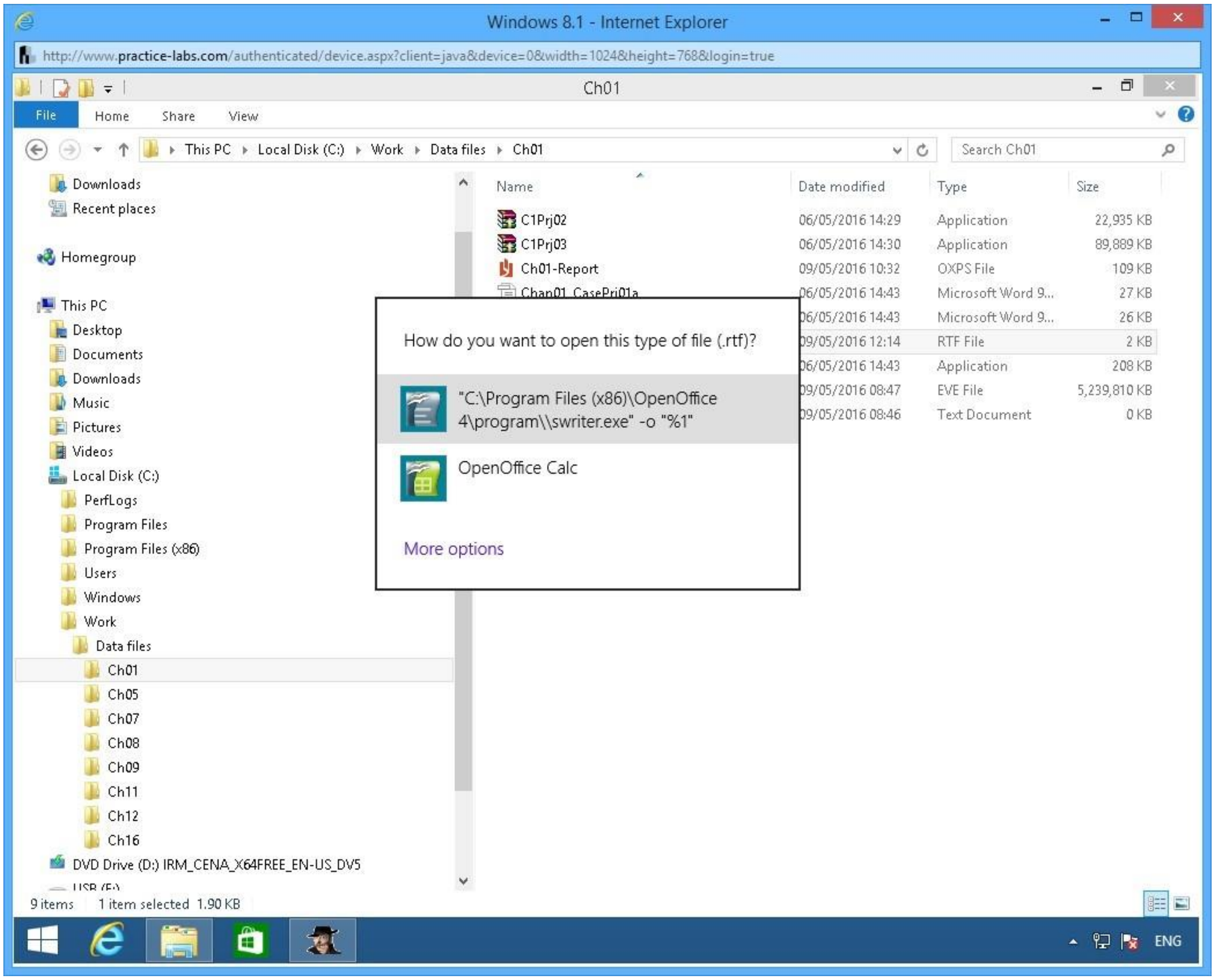
Quay lại hộp thoại **Export** , bấm **OK** .

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Bước 11

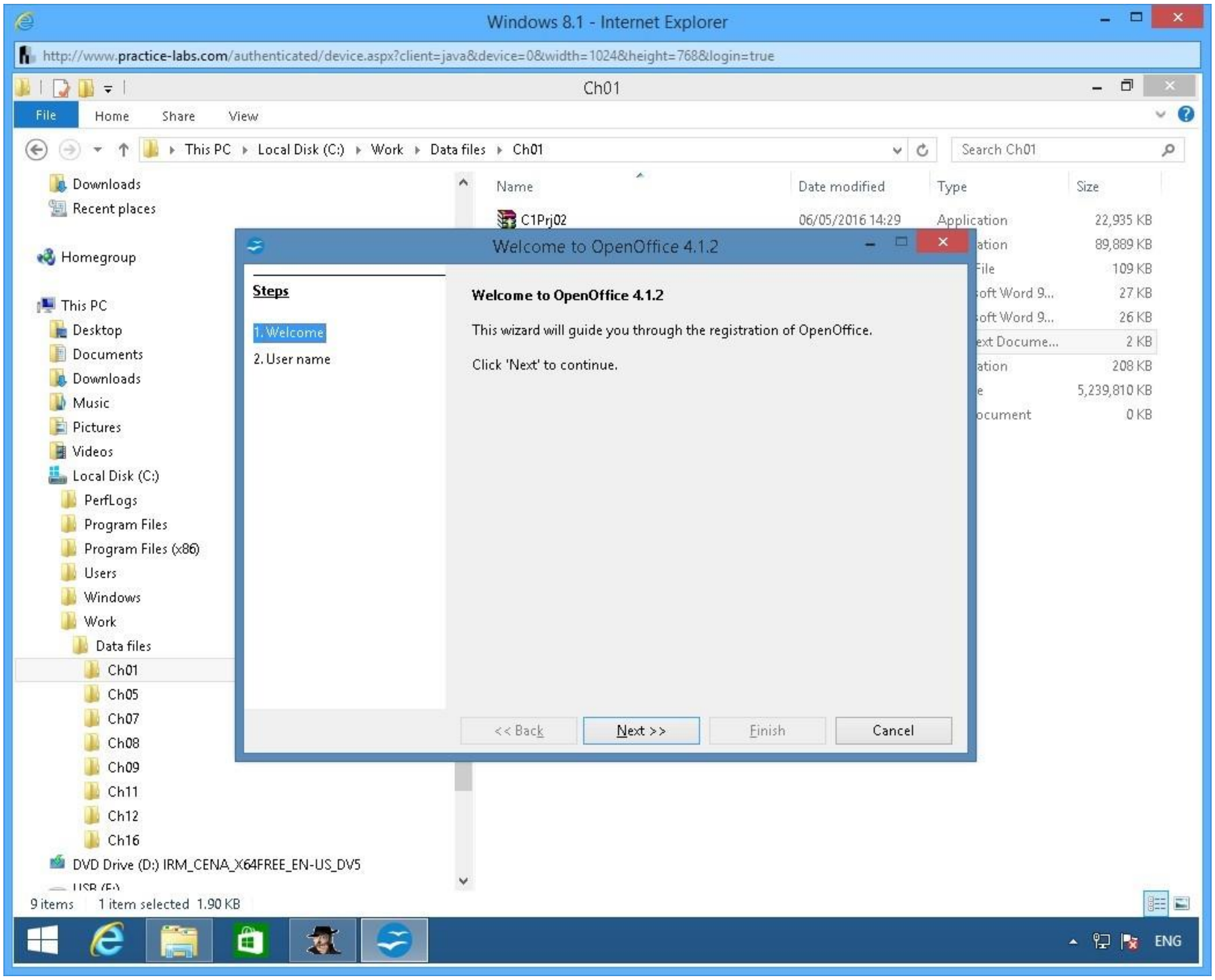
Trên hộp thoại **Làm cách nào bạn muốn mở tệp này** , hãy nhấp vào “ **C: \ Program Files (x86) \ OpenOffice 4 \ program \\ swriter.exe” -o% 1.** ”



Bước 12

Trên hộp thoại **Chào mừng đến với OpenOffice 4.1.2** , bấm **Tiếp theo** .

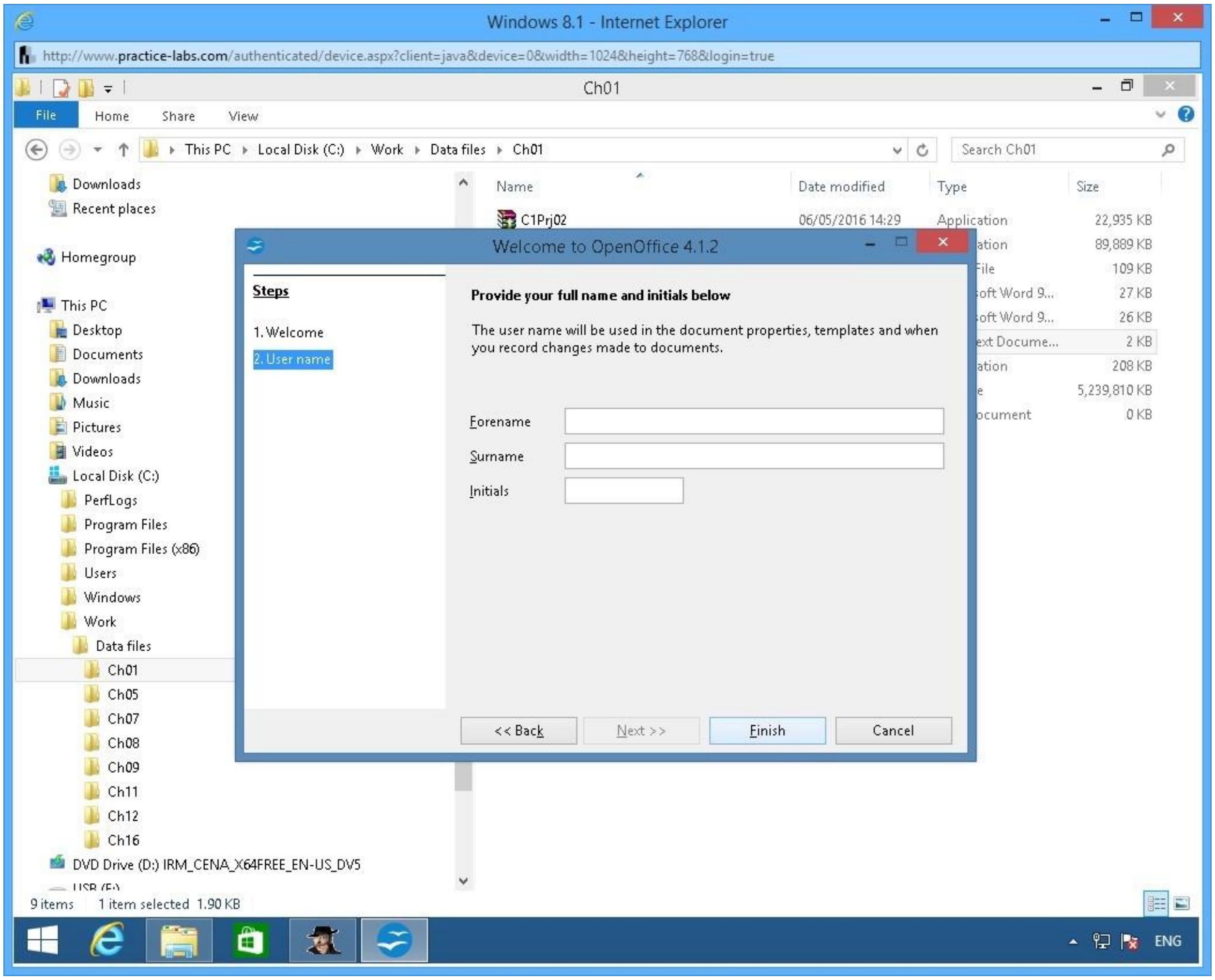
Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo



Bước 13

Trên trang **Cung cấp tên đầy đủ và tên viết tắt của bạn bên dưới** , hãy để trống các trường và nhấp vào **Hoàn tất** .

Hãy hoàn tất các bài thực hành và chụp hình minh họa qua nút Take Screenshot hay Xuất Báo Cáo

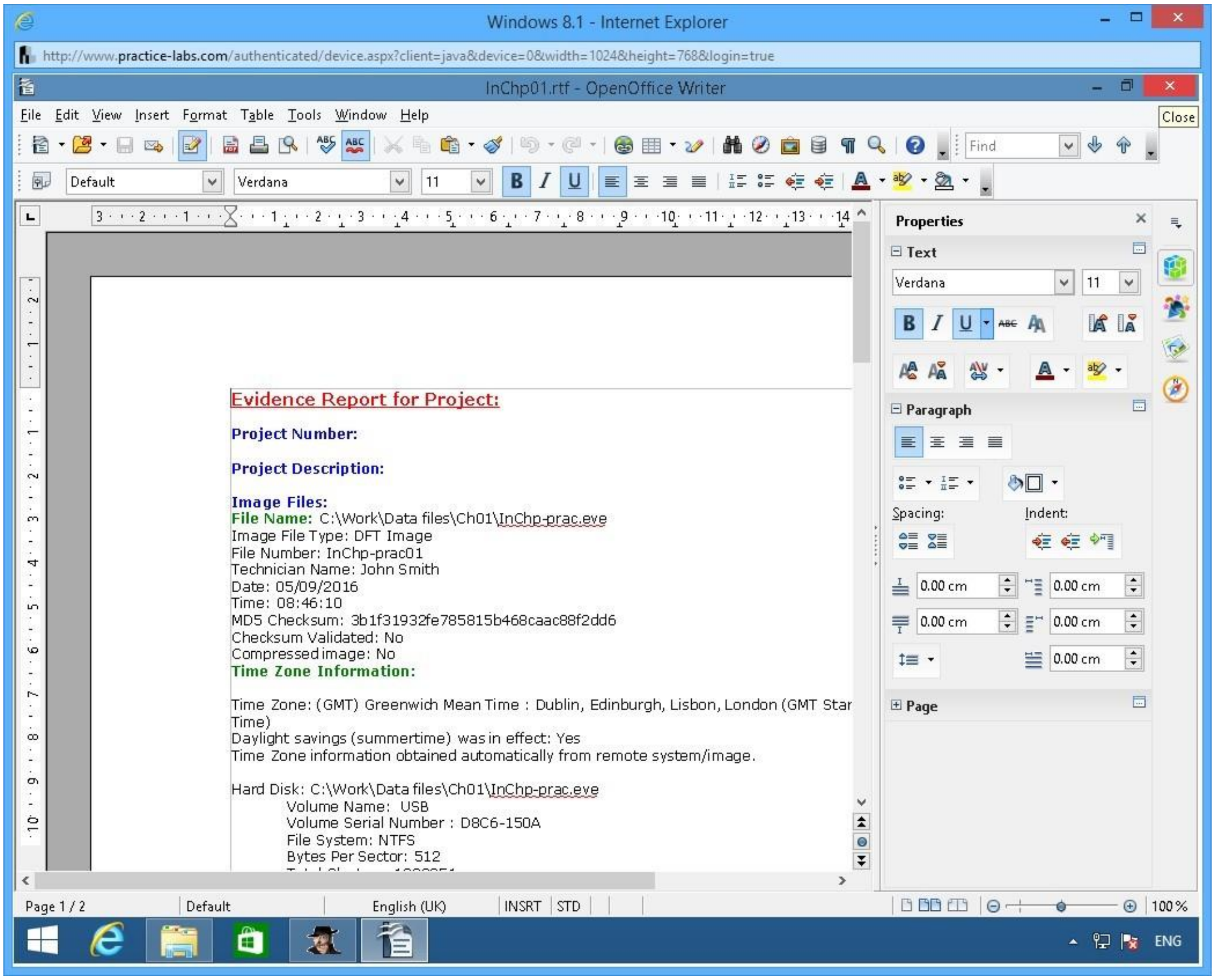


Bước 14

Xem lại Report, đóng ứng dụng **OpenOffice Writer** khi hoàn tất.

Tương tự, nhấp vào **Tệp** , **Thoát** từ menu để thoát khỏi **ProDiscover Basic** .

Hoạt động này hoàn thành phân tích của bạn về ổ USB. Trong phần tiếp theo, bạn học cách hoàn thành một vụ án hay tình huống điều tra. Trong các chương sau, bạn học cách áp dụng nhiều kỹ thuật tìm kiếm và phân tích hơn.



Giữ cho thiết bị được bật nguồn ở trạng thái hiện tại và tiến hành tác vụ tiếp theo.

Dự án thực hành 1-1

Trong các dự án thực hành tiếp theo, hãy tiếp tục làm việc trên máy trạm **PLABWIN810** .

Lưu ý: *Nếu cần, hãy tham khảo hướng dẫn trong chương này và hướng dẫn sử dụng*

ProDiscover, trong C: \ ProgramFiles (x86) \ Technology Pathways \ ProDiscover theo mặc định.

Vụ án trong dự án này liên quan đến một cái chết đáng ngờ. Joshua Zarkan đã tìm thấy xác chết của bạn gái mình trong căn hộ của cô ấy và trình báo. Nhân viên thực thi pháp luật phản ứng đầu tiên đã thu giữ một ổ USB. Một kỹ thuật viên chứng cứ hiện trường vụ án có kỹ năng thu thập dữ liệu đã tạo hình ảnh ổ USB bằng ProDiscover và đặt tên là **daylightTest.eve** . Sau khi thu thập chứng cứ, kỹ thuật viên đã vận chuyển và bảo mật ổ USB và đặt nó vào một tủ đựng vật chứng an toàn tại đồn cảnh sát. Bạn đã nhận được tệp hình ảnh từ thám tử được chỉ định cho vụ án này. Anh

ta hướng dẫn bạn kiểm tra nó và xác định bất kỳ hiện vật chứng cứ nào có thể liên quan đến trường hợp này.

Trong khi xem xét thực hành này, nếu bạn nhận được bất kỳ tài liệu tham khảo nào về thư mục công việc, điều này đề cập đến **c: \ Work \ Data files \ Ch01**.

Để xử lý vụ án này, hãy làm theo các bước sau để đánh giá hình ảnh của ổ USB:

Bước 1

Khởi động **ProDiscover Basic** .

Bước 2

Trong hộp thoại Khởi chạy Hộp thoại, bấm vào tab **Dự án Mới** .

Nhập số dự án. Nếu công ty của bạn không có sơ đồ đánh số tiêu chuẩn, bạn có thể sử dụng ngày theo sau là số đại diện cho trường hợp của ngày đó theo thứ tự, chẳng hạn như 20150124 01.

Bước 3

Nhập **C1Prj01** làm tên dự án, nhập mô tả ngắn gọn về trường hợp, sau đó bấm **Open** .

Bước 4

Để thêm tệp hình ảnh, hãy nhấp vào **Hành động** từ menu, trỏ chuột vào **Thêm** và nhấp vào **Tệp Hình ảnh** .

Bước 5

Điều hướng đến **C: \ Program Files (x86) \ Technology Pathways \ ProDiscover \ Sample Images,** sau đó nhấp vào **daylightTest.eve** và sau đó nhấp vào **Open** .

Nếu hộp thông báo Kiểm tra Hình ảnh Tự động Open ra, hãy bấm **Có** .

Bước 6

Trong chế độ xem dạng cây, hãy nhấp để mở rộng **Chế độ xem nội dung** .

Bấm để mở rộng **Hình ảnh** , sau đó bấm vào tên đường dẫn chứa tệp hình ảnh. Trong khu vực làm việc, hãy để ý các tệp được liệt kê.

Bước 7

Bấm chuột phải vào tệp bất kỳ và bấm **Xem** để khởi động chương trình được liên kết, chẳng hạn như **OpenOffice Writer** hoặc **OpenOffice Calc,** tùy theo chương trình nào áp dụng được. Xem tệp, sau đó thoát khỏi chương trình.

Bước 8

Nếu bạn quyết định xuất tệp, hãy bấm chuột phải vào tệp và bấm **Sao chép tệp** . (Lưu ý: Tạo một thư mục riêng để xuất là một ý tưởng hay để giữ cho các tệp của bạn có tổ chức.)

Trong hộp thoại **Lưu dưới dạng** Open ra, điều hướng đến vị trí bạn muốn lưu tệp, sau đó bấm **Lưu** .

Bước 9

Để lưu dự án để xem sau này, hãy nhấp vào **Tệp** , **Lưu Dự án** từ menu. Tên dự án mặc định là tên bạn đã nhập ở Bước 3. Chọn ổ đĩa và thư mục (ví dụ: WorknChap01nProjects), rồi bấm **Lưu .** Sau khi bạn kiểm tra xong các tệp, hãy thoát khỏi ProDiscover Basic và lưu lại dự án, nếu được nhắc.

Bạn cần xuất bất kỳ tệp nào trong hình ảnh này và đưa chúng cho người điều tra. Ngoài ra, hãy viết một Report ngắn gọn (không quá hai đoạn văn) bao gồm bất kỳ sự kiện nào từ nội dung của dữ liệu được phục hồi. Trong ProDiscover Basic, bạn phải thoát khỏi chương trình trước khi bắt đầu một trường hợp mới.

Dự án thực hành 1-2

Trong các dự án thực hành tiếp theo, hãy tiếp tục làm việc trên máy trạm **PLABWIN810** .

Trong dự án này, bạn làm việc cho một công ty bảo mật CNTT của một tập đoàn lớn. Nhiệm vụ của bạn bao gồm thực hiện điều tra máy tính nội bộ và kiểm tra pháp y số trên hệ thống máy tính của công ty. Bà Jones, một phụ tá của Bộ luật pháp y số yêu cầu bạn kiểm tra ổ USB của một nhân viên đã rời công ty và hiện đang làm việc cho một đối thủ cạnh tranh. Bộ luật lo ngại rằng nhân viên cũ có thể sở hữu dữ liệu nhạy cảm của công ty. Cô Jones muốn biết liệu ổ USB có chứa thứ gì đáng kể hay không.

Ngoài ra, cô ấy thông báo với bạn rằng nhân viên cũ có thể đã truy cập vào tài liệu bí mật vì một đồng nghiệp đã nhìn thấy anh ta truy cập vào máy tính của người quản lý vào ngày làm việc cuối cùng. Các tài liệu bí mật này bao gồm 24 tệp với văn bản là " **đoạn** ". Cô ấy muốn bạn xác định bất kỳ lần xuất hiện nào của các tệp này trên hình ảnh luồng bit của ổ USB.

Để xử lý trường hợp này, bạn sẽ sử dụng tệp có tên là tệp **FATSearchTestImage.eve** trên máy trạm phòng thí nghiệm của mình, sau đó làm theo các bước sau:

Bước 1

Khởi động **ProDiscover** Basic. Trong tab **Dự án Mới** , nhập số dự án, tên dự án **C1Prj02** và mô tả dự án, sau đó bấm Open. Bạn nên có thói quen lưu dự án ngay lập tức, vì vậy hãy nhấp vào Tệp, Lưu Dự án từ menu và lưu tệp trong thư mục công việc **C: \ Work \ Data files \ Ch01** \.

Bước 2

Nhấp vào **Hành động** từ trình đơn, trỏ chuột vào **Thêm** và nhấp vào **Tệp Hình ảnh** .

Điều hướng đến **C: \ Program Files (x86) \ Technology Pathways \ ProDiscover \ Sample Images,** sau đó nhấp và nhấp vào thư mục **FATSearchTestImage.eve** , sau đó nhấp vào **Open** .

Nếu hộp thông báo Kiểm tra **Hình ảnh Tự động** Open ra, hãy bấm **Có** .

Bước 3

Trong chế độ xem dạng cây, hãy nhấp để Mở rộng Chế độ xem **nội dung** , nếu cần.

Bấm để Mở rộng **Hình ảnh** , sau đó bấm vào tên đường dẫn chứa tệp hình ảnh. Trong khu vực làm việc, hãy kiểm tra các tệp được liệt kê.

Bước 4

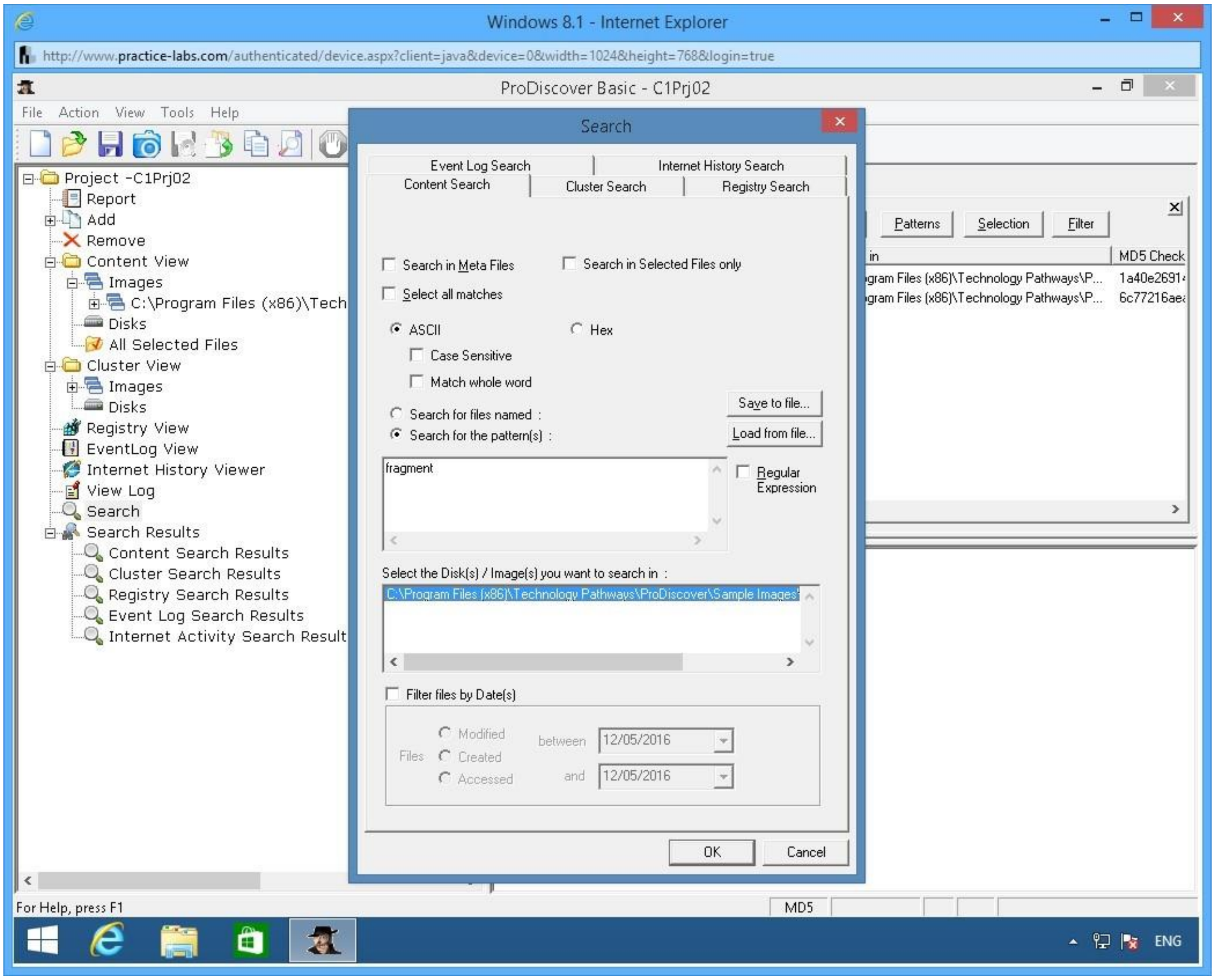
Để tìm kiếm từ khóa “ **phân mảnh** ” , hãy nhấp vào nút trên thanh công cụ **Tìm kiếm** để Open hộp thoại **Tìm kiếm** .

Bước 5

Nếu cần, hãy bấm vào tab **Tìm kiếm Nội dung** , rồi bấm vào nút tùy chọn **ASCII** và nút tùy chọn **Tìm kiếm (các) mẫu** .

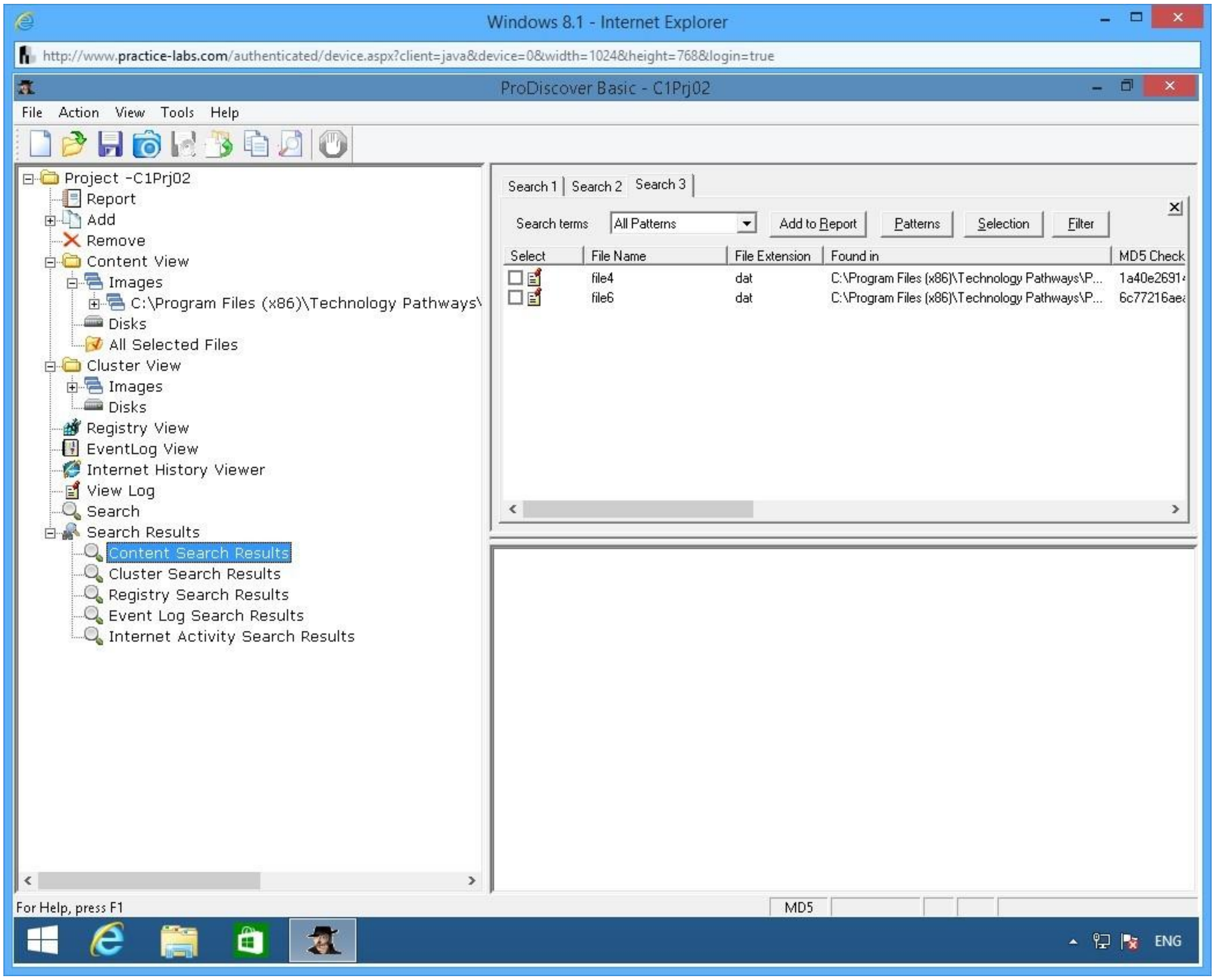
Nhập **phân đoạn** vào hộp danh sách cho các từ khóa tìm kiếm.

Trong **Chọn (các) Đĩa / (các) Hình ảnh bạn muốn tìm kiếm** , hãy bấm vào ổ đĩa bạn đang tìm kiếm rồi bấm **OK** .



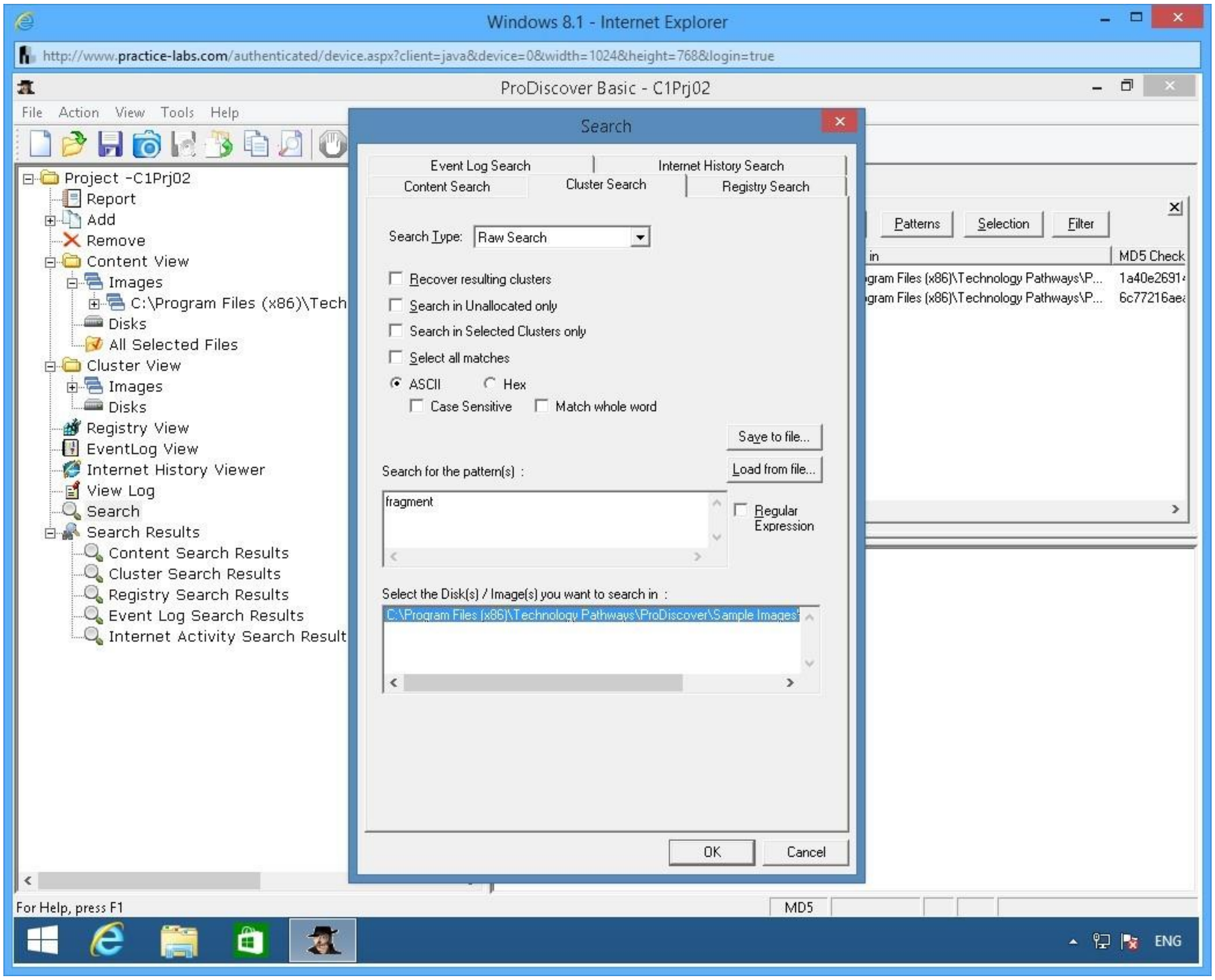
Bước 6

Trong chế độ xem dạng cây, hãy bấm để mở rộng Kết quả tìm kiếm, nếu cần, rồi bấm Kết quả tìm kiếm nội dung để chỉ định loại tìm kiếm. Ảnh chụp màn hình bên dưới hiển thị ngăn kết quả tìm kiếm.



Bước 7

Tiếp theo, mở nút **Tìm kiếm** để truy cập lại hộp thoại **Tìm kiếm** , nhấp vào tab **Tìm kiếm theo cụm** và chạy tìm kiếm tương tự. Lưu ý rằng nó mất nhiều thời gian hơn vì mỗi cụm trên ổ đĩa được tìm kiếm.



Bước 8

Trong chế độ xem dạng cây, bấm **Kết quả Tìm kiếm Cụm** và xem ngăn kết quả tìm kiếm. Hãy nhớ lưu dự án của bạn và thoát khỏi ProDiscover Basic trước khi bắt đầu trường hợp tiếp theo.

Khi bạn hoàn thành, hãy viết một bản ghi nhớ cho cô Jones với thông tin sau: tên tệp mà bạn đã tìm thấy lần truy cập cho từ khóa và nếu lần truy cập xảy ra trong không gian chưa được phân bổ, số cụm.

Đóng ứng dụng **ProDiscover Basic** .

Dự án thực hành 1-3

Trong các dự án thực hành tiếp theo, hãy tiếp tục làm việc trên máy trạm **PLABWIN810** .

Cô Jones thông báo cho bạn rằng nhân viên cũ đã sử dụng thêm một ổ đĩa. Cô ấy yêu cầu bạn kiểm tra ổ đĩa mới này để xác định xem nó có chứa số tài khoản mà nhân viên có thể có quyền truy

cập hay không. Từ khóa 1cro thuộc về phó chủ tịch cấp cao và được sử dụng để truy cập dịch vụ ngân hàng của công ty qua Internet.

Bước 1

Khởi động **ProDiscover Basic** .

Trong tab Dự án Mới, nhập số dự án, tên dự án **C1Prj03** và mô tả ngắn gọn, sau đó bấm **Open** .

Lưu dự án trong thư mục công việc của bạn bằng cách nhấp vào **Tệp** , **Lưu Dự án** từ menu.

Bước 2

Để thêm bằng chứng, hãy nhấp vào **Hành động** từ menu, trỏ chuột vào **Thêm** và nhấp vào **Tệp Hình ảnh** .

Điều hướng đến **C: \ Program Files (x86) \ Technology Pathways \ ProDiscover \ Sample Images** và nhấp vào **FATSearchTestImage.eve** sau đó nhấp vào **Open** .

Bấm **Có** trong hộp thông báo Tự động Kiểm tra Hình ảnh, nếu cần.

Bước 3

Để hỗ trợ điều tra của bạn, bạn có thể muốn xem các tệp đồ họa trên ổ đĩa. Để thực hiện việc này, hãy bấm để mở rộng **Chế độ xem nội dung** trong chế độ xem dạng cây, bấm để Mở rộng **Hình ảnh** , sau đó bấm vào tên đường dẫn chứa tệp hình ảnh.

Bước 4

Bấm vào menu **View** và chọn **Gallery View** .

Cuộn qua các tệp đồ họa trên hình ảnh ổ đĩa. Bạn sẽ cần tìm kiếm trong tất cả các thư mục, có thể mất một chút thời gian. Nếu một tệp được quan tâm, hãy nhấp vào hộp kiểm bên cạnh tệp đó trong cột Chọn. Trong hộp thoại Thêm nhận xét Open ra, hãy nhập mô tả và bấm **OK** . Những ghi chú này được thêm vào Report ProDiscover.

Bước 5

Ổ đĩa này có liên quan đến trường hợp trong Dự án Thực hành 1-2, vì vậy bạn vẫn đang tìm kiếm sự xuất hiện của từ “**fragment** ”. Open hộp thoại Tìm kiếm và lặp lại các Bước từ 5 đến 8 của Dự án Thực hành 1-2 cho ảnh ổ đĩa này. Khi bạn xem kết quả tìm kiếm, hãy nhấp để chọn bất kỳ tệp nào quan tâm (như được mô tả trong Bước 4), thao tác này sẽ Open ra hộp thoại Thêm nhận xét nơi bạn có thể nhập ghi chú.

Bước 6

Tiếp theo, hãy tìm kiếm từ khóa **1cro mà** cô Jones đã đưa cho bạn. Nhấp vào nút trên thanh công cụ **Tìm kiếm** . Nhấp vào tab **Tìm kiếm Nội dung** , nếu cần và nhập **1cro** làm từ khóa tìm kiếm. Bấm để chọn ổ đĩa bạn đang tìm kiếm, sau đó bấm **OK** .

Nhấp vào tab **Tìm kiếm theo cụm** và lặp lại tìm kiếm cho từ khóa. Hãy nhớ chọn bất kỳ tệp nào quan tâm và nhập ghi chú vào hộp thoại Thêm nhận xét.

Hãy nhớ rằng văn bản có thể được tìm thấy trong các tệp đồ họa cũng như trong tài liệu. Nếu kết quả tìm kiếm của bạn không có kết quả nào, bạn có thể phải tìm kiếm riêng các tệp đồ họa và hình ảnh để làm bằng chứng.

Bước 7

Khi bạn hoàn tất, hãy nhấp vào Report trong chế độ xem dạng cây. Cuộn qua Report để đảm bảo rằng tất cả các mục bạn tìm thấy đều được liệt kê.

Bước 8

Tiếp theo, nhấp vào nút Xuất trên thanh công cụ. Trong hộp thoại **Xuất** , bấm vào nút tùy chọn **Định dạng RTF** , nhập **Ch1Prj03Report** vào hộp văn bản Tên tệp, rồi bấm **OK** . (Nếu bạn muốn lưu trữ Report trong một thư mục khác, hãy nhấp vào Duyệt qua và điều hướng đến vị trí mới.)

Bước 9

Viết một bản ghi nhớ ngắn để tóm tắt những gì bạn tìm thấy. Lưu dự án và thoát khỏi ProDiscover Basic.

Đóng ProDiscover Basic.

Dự án thực hành 1-4

Trong các dự án thực hành tiếp theo, hãy tiếp tục làm việc trên máy trạm **PLABWIN810** .

Đôi khi yêu cầu khám phá từ các công ty luật yêu cầu bạn chỉ khôi phục dữ liệu được cấp phát từ đĩa. Dự án này chỉ cho bạn cách chỉ giải nén các tệp chưa bị xóa khỏi hình ảnh.

Bước 1

Khởi động ProDiscover Basic.

Trong tab Dự án Mới, nhập số dự án, mô tả ngắn gọn và tên dự án **C1Prj04** , sau đó bấm **Open** .

Bước 2

Trong chế độ xem dạng cây, bấm để Mở rộng **Thêm** , rồi bấm **Đĩa** . Chọn PhysicalDrive1. Nhập tên duy nhất vào văn bản được cung cấp bên dưới tên đó và nhấp vào **Thêm .**

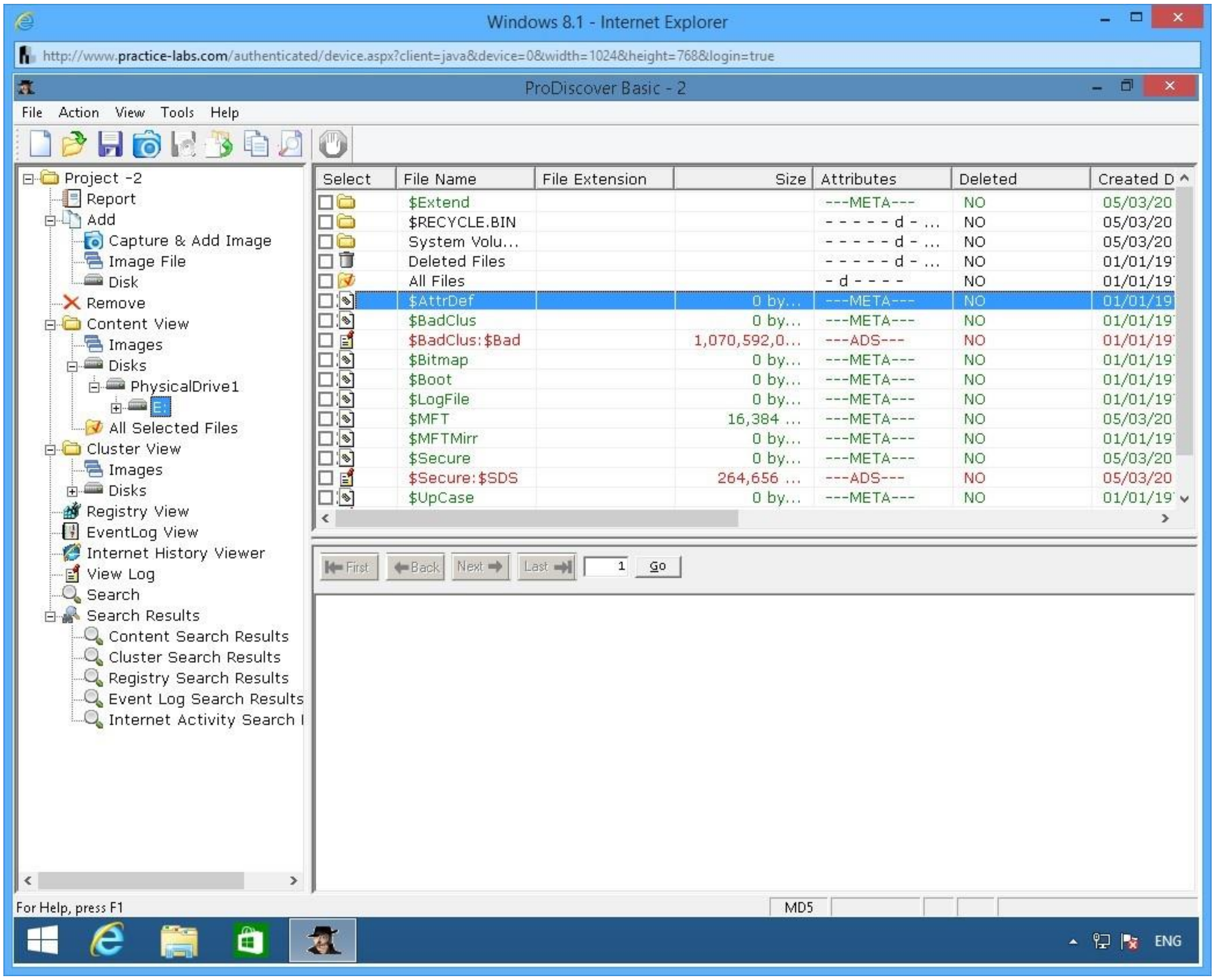
Bấm **Có** trong hộp thông báo Tự động Kiểm tra Hình ảnh, nếu cần. Lưu dự án trong thư mục công việc của bạn.

Bước 3

Trong chế độ xem dạng cây, hãy nhấp để Mở rộng Chế độ xem nội dung, nếu cần. Nhấp để Mở rộng Disks > Physical Drive1 > E. Lưu ý các tệp được hiển thị trong vùng làm việc.

Bước 4

Nhấp vào tiêu đề cột **Đã xóa** để sắp xếp tệp thành các nhóm CÓ và KHÔNG (xem ảnh chụp màn hình bên dưới).



Bước 5

Để trích xuất các tệp được phân bổ từ hình ảnh vào thư mục công việc của bạn, hãy nhấp chuột phải vào từng tệp chứa KHÔNG trong cột Đã xóa và nhấp vào **Sao chép Tệp** .

(Lưu ý rằng trong ProDiscover Basic, không có cách nào để chọn nhiều tệp cùng một lúc. Bạn phải sao chép từng tệp được phân bổ riêng biệt.) Khi bạn hoàn thành, hãy lưu dự án và thoát khỏi ProDiscover Basic.

Dự án thực hành 1-5

Trong các dự án thực hành tiếp theo, hãy tiếp tục làm việc trên máy trạm **PLABWIN810** .

Dự án này là sự tiếp nối từ dự án trước đó; bạn sẽ tạo một Report liệt kê tất cả các tệp chưa được phân bổ (đã xóa) mà ProDiscover tìm thấy.

Bước 1

Khởi động ProDiscover Basic. Tạo một dự án mới.

Bước 2

Nhập số dự án tùy chỉnh của bạn.

Trong tên tệp dự án, nhập **C1Prj04** và bấm **OK** .

Bấm **Có** trong hộp thông báo Tự động Kiểm tra Hình ảnh, nếu cần.

Bước 3

Nhấp vào **Hành động** và chọn **Thêm> Đĩa** …

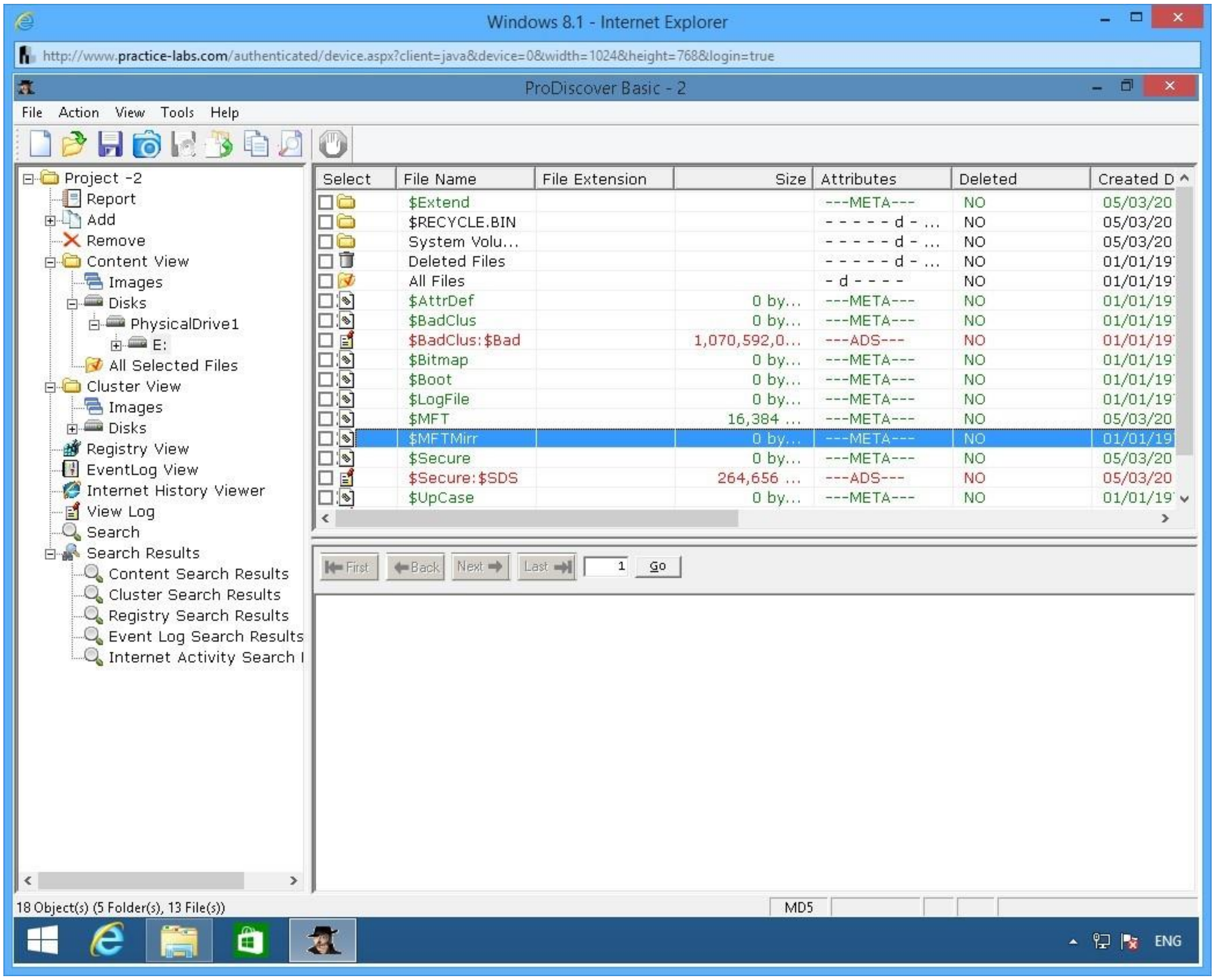
Chọn **PhysicalDrive1** , nhập tên duy nhất vào hộp văn bản. Nhấp vào **Thêm** .

Bước 4

Mở rộng **Content View > Disks > PhysicalDrive1** rồi bấm Ổ đĩa **E.**

Bước 4

Nếu cần, hãy sắp xếp lại các tệp trong vùng làm việc bằng cách bấm vào tiêu đề cột Đã xóa. Bấm vào hộp kiểm trong cột Chọn bên cạnh bất kỳ tệp được phân bổ nào. Khi bạn nhấp vào từng hộp kiểm, hộp thoại Thêm nhận xét sẽ Open ra, tại đây bạn có thể nhập mô tả của từng tệp.



Bước 5

Trong hộp văn bản nhận xét của Người điều tra, hãy thêm chú thích rằng tệp nằm trên đĩa và cho biết loại tệp của nó, chẳng hạn như tài liệu Word hoặc tệp hình ảnh (ví dụ: .jpeg hoặc .gif). Đảm bảo nhập nội dung có ý nghĩa bằng cách kiểm tra tệp trước.

Bước 6

Khi bạn hoàn tất, hãy nhấp vào Report trong chế độ xem dạng cây. Nếu bạn hài lòng, hãy xuất Report bằng cách nhấp vào nút Xuất trên thanh công cụ. Trong hộp thoại Xuất, hãy chọn tùy chọn định dạng bạn muốn, nhập C1Prj05Report vào hộp văn bản Tên tệp, rồi bấm OK. Lưu dự án và thoát khỏi ProDiscover Basic.

Dự án thực hành 1-6

Trong các dự án thực hành tiếp theo, hãy tiếp tục làm việc trên máy trạm **PLABWIN810** .

Trong dự án này, một điều tra viên khác yêu cầu bạn kiểm tra hình ảnh và tìm kiếm tất cả các lần xuất hiện của các từ khóa sau:

- plabwin810
- vỏ sò

Bước 1

Khởi động ProDiscover Basic. Trong tab Dự án Mới, nhập số dự án, mô tả ngắn gọn và tên dự án, sau đó bấm Open.

Bước 2

Trong chế độ xem dạng cây, hãy nhấp để Mở rộng **Thêm** và nhấp vào **Đĩa** .

Chọn **PhysicalDrive1,** sau đó nhập tên duy nhất vào hộp văn bản rồi bấm **Open** .

Bấm **Có** trong hộp thông báo Tự động Kiểm tra Hình ảnh, nếu cần. Lưu dự án trong thư mục công việc của bạn.

Bước 3

Nhấp vào nút trên thanh công cụ **Tìm kiếm** . Trong hộp thoại Tìm kiếm, nhập tất cả các từ khóa vào hộp danh sách (đặt mỗi từ khóa trên một dòng riêng biệt), bấm để chọn ổ chứa hình ảnh và bấm OK.

Bước 4

Kiểm tra các tệp trong ngăn kết quả tìm kiếm. Chọn những cái nhìn thú vị và nhập ghi chú vào hộp thoại Thêm nhận xét.

Bước 5

Tạo Report và xuất nó, như đã giải thích trong các dự án trước. Lưu dự án và thoát khỏi ProDiscover Basic.

Tóm lược

- Pháp y số kỹ thuật số áp dụng quy trình pháp y số cho bằng chứng kỹ thuật số. Quá trình này liên quan đến việc tích lũy và phân tích thông tin kỹ thuật số một cách có hệ thống để sử dụng làm bằng chứng trong các vụ án dân sự, hình sự và hành chính. Pháp y số kỹ thuật số khác với pháp y số mạng và phục hồi dữ liệu ở phạm vi, kỹ thuật và mục tiêu.
- Các luật liên quan đến bằng chứng kỹ thuật số được thiết lập vào những năm 1970.
- Để trở thành một nhà điều tra pháp y số kỹ thuật số thành công, bạn phải làm quen với nhiều nền tảng máy tính. Để bổ sung kiến thức của bạn, hãy phát triển và duy trì liên lạc với các chuyên gia máy tính, mạng và điều tra.

- Các nhà điều tra cần các máy trạm chuyên dụng để kiểm tra bằng chứng kỹ thuật số, bao gồm các khoang bổ sung cho ổ đĩa bằng chứng, phần mềm pháp y số và trình chặn ghi.
- Các cuộc điều tra khu vực công và khu vực tư nhân khác nhau, ở chỗ các cuộc điều tra khu vực công thường yêu cầu lệnh khám xét trước khi thu giữ bằng chứng kỹ thuật số. Tu chính án thứ tư đối với Hiến pháp Hoa Kỳ và luật tương tự ở các quốc gia khác áp dụng cho việc khám xét và thu giữ của chính phủ. Trong các cuộc điều tra khu vực công, bạn tìm kiếm bằng chứng để hỗ trợ các cáo buộc tội phạm. Trong quá trình điều tra khu vực tư nhân, bạn tìm kiếm bằng chứng để hỗ trợ các cáo buộc vi phạm chính sách, lạm dụng tài sản và trong một số trường hợp là khiếu nại hình sự.
- Các biểu ngữ cảnh báo nên được sử dụng để nhắc nhở nhân viên và khách về chính sách của công ty về việc sử dụng máy tính, e-mail và Internet.
- Các công ty nên xác định và giới hạn số lượng người yêu cầu được ủy quyền có thể bắt đầu điều tra.
- Các nhà điều tra pháp y số kỹ thuật số phải duy trì hành vi chuyên nghiệp để bảo vệ uy tín của họ.
- Luôn sử dụng một cách tiếp cận có hệ thống cho các cuộc điều tra của bạn. Thực hiện theo danh sách kiểm tra trong chương này như một hướng dẫn cho trường hợp của bạn.
- Khi lập kế hoạch cho một trường hợp, hãy tính đến bản chất của trường hợp, hướng dẫn từ người yêu cầu, những công cụ và kiến thức chuyên môn bổ sung nào bạn có thể cần và cách bạn thu thập bằng chứng.
- Các vụ án hình sự và vi phạm chính sách của công ty nên được xử lý theo cùng một cách để đảm bảo rằng bằng chứng chất lượng được trình bày. Cả hai vụ án hình sự và vi phạm chính sách của công ty đều có thể ra tòa.
- Khi bạn bắt đầu một vụ án, có thể có những thách thức không lường trước được mà không rõ ràng khi áp dụng một cách tiếp cận có hệ thống cho kế hoạch điều tra của bạn. Đối với tất cả các cuộc điều tra, bạn cần lên kế hoạch dự phòng cho mọi vấn đề bất ngờ mà bạn có thể gặp phải.
- Bạn nên tạo một biểu mẫu lưu giữ bằng chứng tiêu chuẩn để theo dõi chuỗi lưu giữ bằng chứng cho trường hợp của bạn. Có hai loại biểu mẫu: biểu mẫu nhiều chứng cứ và đơn chứng cứ.
- Các cuộc điều tra lạm dụng Internet yêu cầu kiểm tra dữ liệu nhật ký máy chủ.
- Đối với các trường hợp đặc quyền của luật sư-khách hàng, tất cả các thông báo bằng văn bản phải có nhãn tiêu đề cho biết rằng thông tin liên lạc đặc quyền và sản phẩm công việc bí mật.
- Bản sao theo luồng bit là bản sao từng bit của đĩa gốc. Bạn nên sử dụng bản sao, bất cứ khi nào có thể, khi phân tích bằng chứng.
- Luôn ghi nhật ký để ghi lại chính xác những gì bạn đã làm khi xử lý bằng chứng.
- Bạn nên luôn tự phê bình công việc của mình để xác định xem bạn đã thực hiện những cải tiến nào trong mỗi trường hợp, điều gì có thể đã được thực hiện theo cách khác và cách áp dụng những bài học đó cho các trường hợp sau này.

Biên soạn bởi : Nguyen Tran Tuong Vinh – Dai Ngoc Son – Minh NG

Hiệu chỉnh : Mina Quỳnh Viên

Chương trình đào tạo CHFI Online & Thực Hành Trên Lab Thật Trực Tuyến

https://akademy.edu.vn/course/chuong-trinh-dao-tao-chfi-v9/